Subject: RE: Sunshine Law Request (MO-SOS-23-0911)
Date: Friday, September 29, 2023 at 4:15:43 PM Eastern Daylight Time
From: CustodianOfRecords
To: AO Records
CC: CustodianOfRecords

EXTERNAL SENDER

Mariuxi Pintado,

As custodian of records for the Missouri Secretary of State, your Sunshine request has been forwarded to my attention. Below is a Citrix Sharefile link to the documents requested, please download the file within 7 days as the link will expire. As this was a small effort the cost associated with gathering these records is de minimis, please note future request may have a cost associated.

https://mosecretaryofstate.sharefile.com/d-s9760a2016c894ef9a8851654f454fb0c

Scott R Clark **| Deputy Chief of Staff**
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65101

From: SOSMain <sosmain@sos.mo.gov>
Sent: Tuesday, September 26, 2023 4:22 PM
To: CustodianOfRecords <CustodianOfRecords@sos.mo.gov>
Subject: FW: Sunshine Law Request (MO-SOS-23-0911)

From: AO Records <records@americanoversight.org>
Sent: Tuesday, September 26, 2023 4:18 PM
To: SOSMain <sosmain@sos.mo.gov>
Subject: Sunshine Law Request (MO-SOS-23-0911)

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Custodian of Records:

Please find attached a request for records under Missouri's Sunshine Law.

Sincerely,

Mariuxi Pintado | (she/hers)
Senior Paralegal | American Oversight

AMERICAN OVERSIGHT

records@americanoversight.org
www.americanoversight.org | @weareoversight

Sunshine Law Request: MO-SOS-23-0911

From: kmuthig@eac.gov
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 8/9/2023 12:00:53 PM
Subject: August Newsletter: EAC Updates & Events

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

UPDATES & EVENTS

AUGUST 2023 NEWSLETTER

Highlights from this month's newsletter include:

- **National Poll Worker Recruitment Day is August 23!**
- **New Election Cybersecurity Allocability Underfunding Decision Policy**
- **Latest EAC Resources**
- **Blogs and Videos from the EAC Commissioners on Elections in College Communities, Mental Health, and the Americans with Disabilities Act**
- **Recaps of the EAC Data Summit, LLC Annual Meeting, and EAC Public Meeting on Voter Outreach and Engagement**
- **Upcoming Event EAC Public Meeting on Voting Accessibility scheduled for September 6**

AMERICAN OVERSIGHT

National Poll Worker Recruitment Day is August 23!

The EAC's third annual National Poll Worker Recruitment Day will be held on Wednesday, August 23, 2023. State and local election officials, civic organizations and others can use this national awareness day to encourage Americans to sign up to become poll workers in their communities for upcoming elections.

To help participate in this day, the EAC has created a highly customizable social media toolkit at **HelpAmericaVote.gov**. The toolkit is easily editable to meet the needs of your jurisdiction or organization. The sample posts cater to both Twitter/X and Facebook.

The EAC also offers a **Poll Worker Recruitment Lookup Tool** to help people interested in signing up to be poll workers find information for their local election offices. If you are an election official, please make sure to review your election office's poll worker information in the tool. Please send any updates to **helpamericavote@eac.gov**.

The EAC's Local Leadership Council (LLC) Holds its First In-Person Annual Meeting

In late July, the EAC's Local Leadership Council (LLC) held its first in-person annual meeting since the board was established in June 2021. The 100-member board of election officials from across the country gathered for the two-day meeting in Washington, D.C.

AMERICAN OVERSIGHT

The meeting included moderated discussions on topics such as training and workforce development, looking ahead to 2024, and making the LLC an effective advisory board. Additionally, LLC members elected their first executive officers.

Learn more about the LLC.

New Election Cybersecurity Allocability Underfunding Decision Policy

In July 2023, the U.S. Election Assistance Commission (EAC) voted unanimously to consider allowable cybersecurity enhancements direct costs and allow full allocability under HAVA Section 101(b)(1)(F) of HAVA when the costs are reasonable and necessary and when the cost is incurred specifically for the purpose of benefitting election administration. The vote does not change the applicability of the Uniform Guidance (2 CFR Part 200) to EAC grant funding.

In accordance with the **Commissioners' decision**, the EA Office of Grants Management, in consultation with the Office of General Counsel, shall provide guidance on how states may attest and document that expenditures qualify as direct costs for the purpose of allocation. Written guidance is forthcoming and will be posted on the EAC Website at **www.eac.gov/grants/grants-guidance**. Questions on this decision must be directed to the Office of Grants Management at **grants@eac.gov**.

LATEST EAC RESOURCES

New Study on Accessibility of Elections for Americans with Disabilities

The EAC, in partnership with Rutgers University, released a pair of reports examining voting accessibility and disability turnout in the 2022 election. The agency worked with Professors Lisa Schur, Douglas Kruse, and Mason Ameri of the Program for Disability Research at Rutgers University to conduct the study.

The researchers focused on voter accessibility in the 2022 election, comparing the results to the same post-election surveys that were conducted in 2020 and 2012. The survey covered topics such as voter turnout, difficulties voting, the need for assistance in voting, voting methods, and treatment by election officials. The researchers also analyzed 2022 voter turnout using U.S. Census data. The findings are critical for election officials who continuously work to meet the needs of their jurisdictions and make voting accessible to all eligible voters.

The reports and other information for **Disability and Voting Accessibility in the 2022 Elections** can be found on the EAC's website. For a quick look at the study, you can also check out the EAC's new blog post on the study at **Understanding Voting Accessibility in the 2022 Elections**.

60 Second Security Series on Physical Security

The EAC created this 60 Second Security Series to help election officials quickly identify and address potential security issues. Each topic includes a brief description, a list of security measures, and potential funding sources for making these improvements. The following resources discuss physical security measures.

- **Personal Security**: Election officials can use the proactive steps in this resource to improve their personal security, such as documenting and reporting every threat and developing a working relationship with federal, state, and local law enforcement.

- **Building Access**: Building access refers to the process of allowing or denying individuals access to enter specific physical facilities. Election officials, who are often responsible for maintaining the security of multiple facilities, may use this checklist to help secure an elections office, secure storage areas, equipment warehouses, or rooms that contain sensitive election items.

- **Deploying Assets**: Election administration requires deploying critical systems within the elections office, as well as in the field at polling locations, satellite offices, or mobile voting units. Election officials can use this resource to address security concerns

AMERICAN OVERSIGHT

- related to deploying assets.

More information about these and other election security best practices can be found at eac.gov/election-officials.

State Elections Policies Data Map

Because election policies differ by state, the EAC created an interactive map to quickly show how state policies and procedures vary. These include policies regarding:

- State Election Officials
- Local Election Officials
- Voter Registration
- In-Person Voting
- Voting by Mail
- Post-Election Processes

The data included in this map was compiled by the National Conference of State Legislatures (NCSL), as of September 8, 2022.
Check out the interactive map and view the full dataset.

Electronic Poll Book Report

Electronic poll books (e-poll books) are central to the in-person voting experience in a growing number of jurisdictions. Election officials have leveraged e-poll books to streamline the check-in process, reduce errors, automate ballot issuing, and collect and display critical data. This report provides information on increasing e-poll book adoption, functions e-poll books fulfill, and applicable state laws and regulations. Understanding the current e-poll book environment enables further assessment of risks, mitigation measures, best practices, and information gaps that require further research.

Read and download the E-Poll Book Report and **view State Certification Requirements for Electronic Poll Books**

NEW VIDEOS AND BLOGS FROM THE EAC COMMISSIONERS

EAC Commissioner Ben Hovland Spotlights Election Administration in College Towns

Commissioner Hovland hosted a panel with eight election officials about administering elections in college towns or jurisdictions with significant student populations. The panel discussed issues and challenges faced by college-aged voters in those locations, voter education and participation efforts, registration for out-of-state students versus in-state students, navigating those different rules across states, and more.

Read the blog and watch the video.

EAC Commissioner Thomas Hicks Interviews Clearinghouse Award Winners for Voter Accessibility Programs

In recognition of the 33rd anniversary of the Americans with Disabilities Act, Commissioner Thomas Hicks held a discussion with election officials Kevin Dragotto from Dubuque County, Iowa; and Antone White and Matt Kelly from Franklin County, Ohio, about their offices' **2022 Clearinghouse Award-winning voter accessibility programs**.

Mr. Dragotto highlighted the Dubuque County Auditor's Office's strategic partnership with the Dubuque County Disabilities Council. After assessing polling locations on Election Day, the partnership was able to determine that small changes like better placement of curbside voting signs, larger laminated elevator signs, and word changes could help improve the voting experience for all.

Mr. White and Mr. Kelly spoke about the Franklin County Board of Elections Early Vote Center's ADA Station, which is located directly inside of the center's main entrance and is equipped with seating so that voters do not have to stand or walk far to use voting equipment. It initially consisted of two check-in stations and three ADA accessible voting kiosks. Due to its popularity, the station was expanded to 12 additional kiosks.

Watch the full discussion.

EAC Commissioner Ben Hovland had a Conversation with Jason Kander on Elections and Mental Health

Commissioner Hovland interviewed Jason Kander, a military veteran and former Missouri Secretary of State, about mental health and how it relates to elections.

Mr. Kander shared his story about his post-traumatic stress disorder, emphasized how everyone has their own struggles, and underlined the importance of sharing experiences with others.

Read the blog and watch the video.

EAC EVENTS RECAP

The EAC Hosts a Public Meeting on Voter Education and Engagement

On August 2, the EAC hosted an in-person public meeting on how election officials can improve education and outreach efforts ahead of the EAC's **Poll Worker Recruitment Day** on August 23.

During the meeting, EAC Commissioners moderated three panels on innovation in voter outreach and engagement, voter education strategies

AMERICAN OVERSIGHT

and ideas for 2024, and the EAC's resources on poll worker recruitment. Panelists included state and local election administrators from Delaware, Montgomery County, Maryland, and Paulding County, Georgia. They were joined by professors from Mississippi State University and Connecticut College, who are leading the EAC's Voter Education Project.

EAC staff also served as panelists to discuss the agency's poll worker resources as well as the agency's College Poll Worker Grant Program—funded for the first time since 2010.
Watch the full event.

The EAC Data Summit Highlights How the U.S. Voted in the 2022 Midterms

On July 19, the EAC held a Data Summit featuring a review of the **Election Administration and Voting Survey (EAVS)** report, the nation's most comprehensive source of election administration data. During the Data Summit, election administrators, EAC staff, and election subject matter experts discussed how voting and election administration have changed since the last midterm election in 2018, the last presidential election in 2020, and how this information can be used to prepare for the 2024 presidential election.

Watch the full event.

SAVE THE DATE

AMERICAN OVERSIGHT

The EAC to Hold a Public Meeting on Voting Accessibility on September 6

On September 6, the EAC will hold a public meeting on breaking down accessibility and language barriers to voting. The meeting, which will be held at the agency's DC office, will include election officials, subject matter experts, and other stakeholders. It will also highlight the EAC's accessibility and language resources for voters and election officials, such as best practices guides, new research, and a first-of-its-kind video training series. This meeting will be live streamed on the **EAC's YouTube channel**.

Please register on the event page if you plan to attend in person.

U.S. Election Assistance Commission

633 3rd Street NW, Suite 200 • Washington, DC 20001

www.eac.gov

Were you forwarded this newsletter? Sign up here.

© 2023

This email was sent to chrissy.peters@sos.mo.gov
U.S. Election Assistance Commission, 633 3rd Street NW, Suite 200, Washington, D.C. 20001, United States
Unsubscribe

AMERICAN OVERSIGHT

From: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Date: 6/22/2023 9:30:20 AM
Subject: RE: Subcommittee and Working Group Updates
Attachments: [EXTERNAL] *** IMPORTANT - Please Read ***: Data Sharing Working Group - State Profiles Survey.msg

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good morning!

I hope you all had a nice weekend. I've heard from 10 states so far. I plan to send an email to all cybersecurity points of contact this afternoon. If you have not yet sent your point of contact and wish to do so, please send me their contact information by 3:00 p.m. EST.

Also, reminder the survey is due on Thursday, June 29! Reattaching Dave's email above.

Thanks!
Mandi

From: Grandjean, Amanda
Sent: Monday, June 12, 2023 10:18 AM
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Cc: Burns, Kimberly <kburns@OhioSOS.Gov>
Subject: RE: Subcommittee and Working Group Updates

Good morning all,

I hope you had a good weekend. Please send your agency's cybersecurity point of contact so that we can start communications with them regarding the secure transfer, retention, and destruction of data.

Thanks,
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

From: Grandjean, Amanda
Sent: Monday, June 5, 2023 3:15 PM
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Subject: Subcommittee and Working Group Updates

Good afternoon all,

I hope you had a great weekend. We had several very productive meetings last week. Thank you to all that actively participated in moving the goal forward. Below is a summary of the meetings last week:

AMERICAN OVERSIGHT

Data Sharing Specifications Subcommittee Meeting Update

On Thursday, June 1, 2023, the Data Sharing Specifications Subcommittee met to discuss the survey that Dave Tackett put together and presented to the group. It was a great conversation that led to several additions to and refinements of the survey. The survey will be used to collect relevant information from each state. This survey will be used to continue to develop the template MOU more comprehensively. Dave will circulate a draft of the survey to the group when it is in a good place to do so. Thanks, Dave, for your leadership! Please let Dave know ASAP if you have any additions to the survey.

We also decided that there needs to be a dedicated group of CISOs/cybersecurity professionals from our offices connected via email to discuss the secure data sharing requirements. **Please respond to this email with your office's cybersecurity point of contact's information** so that we can get this work started on a parallel track to the rest of the work that we are all doing.

Legal MOU Subcommittee Update

The Legal MOU Subcommittee did not meet last week. I don't know about you, but I certainly don't want to have a meeting just for the sake of having a meeting. I've received comments from only about two states now on the template MOU. If you have additional MOUs that you can share with the group or comments to the reattached draft template MOU, please let us know asap. We will continue to plug in data specification language as the Data Sharing Specification Subcommittee builds out the requirements.

Working Group Update

On Friday, June 2, 2023, the Data Sharing Working Group met to discuss subcommittee updates, provide state to state updates, and strategize about next steps. High level notes are set forth below:

- Texas let us know that their legislature passed a bill that would require them to leave ERIC.
- West Virginia discussed conversations they are having with their office of vital statistics regarding death record data. For anyone who is interested, I am happy to provide you with more information regarding how we utilize STEVE data in Ohio.
- Virginia let the group know that they are actively working with their neighboring states to enter into agreements.
- We also discussed leveraging data from our BMVs/DMVs that receive licensure cancellation data from other states to identifying cross-state movers.
- There was discussion about potentially getting NCOA data from the BMV/DMV. If any state is already doing this, please let the group know.
- The group discussed the Limited Access Death Master File Download ("LADMF"). Attached are the instructions and certification documents regarding how to become a certified recipient. You can also access themhere. South Carolina mentioned that they have access to this data via their state data center.
- We also discussed NCOA vendors. Tennessee noted that they have used Melissa Data for NCOA and that Melissa Data also has access to death records from the social security administration.
- Alabama mentioned that they are utilizing a vendor to help them become a certified recipient of this data.
- Ohio continues to have conversations with vendors in the private sector including IBM. We also learned about Thomas Reuters Clear. We can discuss this at our meeting later this week (Friday, June 9, 2023 at 10 a.m. EST).

Please let me know if I missed any notes! Additionally, if you have any questions, please feel free to give me a call.

Thanks!
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

AMERICAN OVERSIGHT

From: David Tackett <dtackett@wvsos.com>
To:
Date: 6/16/2023 3:39:40 PM
Subject: [EXTERNAL] *** IMPORTANT - Please Read ***: Data Sharing Working Group - State Profiles Survey
Attachments: VDSC_TB_final.pdf

******Secretary of State Security Notice******
This e-mail is from an external source. Think before you click links or open attachments.

Ladies and Gentlemen

You are receiving this email because you have shown interest in participating in a voter data sharing cooperative.
As part of this ongoing effort, please find below **a link to a brief survey** that will begin the collection of information to build a profile for your State.
This profile is intended to inform other States about the characteristics surrounding your State as a data sharing partner, including the subject matter contacts, available data, and governance frameworks.

https://www.surveymonk [redacted]

If you are not the best recipient, please share out to the appropriate team member.
We ask that you **complete the survey prior to Thursday, June 29, 2023**, when we plan to review the responses in our next *Data Transport and Format Working Group* meeting.
The attached PDF should offer some additional guidance to your responses, but if you have any questions, do not hesitate to reach out to me or another member of the working group(s).

Thanks in advance for your interest and participation in this laudable effort.
Take good care.

Dave

State Capitol Building
Charleston, WV 25305

Dave Tackett
Chief Information Officer
West Virginia Secretary of State's Office
304-558-6000 (office)
304-356-2670 (direct)
304-549-4420 (mobile)

Email correspondence to and from this email address is subject to the West Virginia Freedom of Information Act and may be disclosed, in whole or in part, to third parties by an authorized State official. It may also be privileged or otherwise protected by work product immunity or other legal rules. Unauthorized disclosure of health, legally privileged, or otherwise confidential information, is prohibited by law. If you have received this email in error, please notify the sender immediately and delete all records of this email.

AMERICAN OVERSIGHT

Voter Data Share Cooperative

TB - TECHNICAL BULLETIN	TB Number: **TB-VDSC-001**
Subject: **State Profile Appendix**	Revised: **06/16/2023**
	Author: Dave Tackett

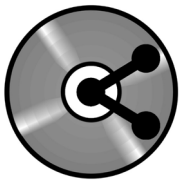
BACKGROUND

This bulletin serves to add supplemental definition to the information solicited in the 'State Profile' survey. *NOTE*: This is **not** intended to be an exhaustive list of fields and/or formats, but rather a quick start to determining the profiles of States interested in sharing this data.

Question	Description or Additional Detail	Likely or Suggested Format
2. Primary Policy Contact	Decision maker as it relates to the administration of Elections	*see survey*
3. Primary Technical Contact	Practitioner as it relates to data logistics	*see survey*
4. Primary Cybersecurity Contact	Practitioner as it relates to data security	*see survey*
6. Import/Export data format	Capabilities and/or preferences of your State	*see survey*
Field Name	**Description or Additional Detail**	**Likely or Suggested Format**
Is the data field available from your State?	**Is the data field considered shareable / part of the public record?**	**Do you have an alternate term for the data field?**
Unique ID	Typically the Voter ID	alphanumeric string
Source ID	Identifier, if different from Unique ID	alphanumeric string
Local Jurisdiction	County/Town/Etc.	alphanumeric string
Registration Effective Date	Date the voter's registration became effective in Jurisdiction	Date (YYYY-MM-DD)
Voter Status	Active/Inactive/Cancelled/Etc.	alphanumeric string

Feedback or Questions to: **dtackett@wvsos.gov**

AMERICAN OVERSIGHT

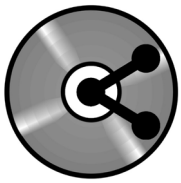


Voter Data Share Cooperative

Field Name	Description or Additional Detail	Likely or Suggested Format
Last Voter Activity Date	Date of the last voter-initiated engagement	Date (YYYY-MM-DD)
Gender	Male/Female/Unknown/Etc.	alphanumeric string
Date of Birth	Voter's date of birth	Date (YYYY-MM-DD)
First Name		alphanumeric string
Middle Name		alphanumeric string
Last Name		alphanumeric string
Former Last Name	(*if applicable*) Maiden/Etc.	alphanumeric string
Suffix		alphanumeric string
Residence Address House No.		alphanumeric string
Residence Address Street		alphanumeric string
Residence Address Street		alphanumeric string
Residence Address Street 2		alphanumeric string
Residence Unit	Apt./Rm./Lot/Etc.	alphanumeric string
Residence Address City		alphanumeric string
Residence Address State		char (2)
Residence Address Zip		numeric (5)
Residence Address Zip+4		numeric (4)
Mailing Address House No.		alphanumeric string
Mailing Address Street		alphanumeric string
Mailing Address Street 2		alphanumeric string
Mailing Unit	Apt./Rm./Lot/Etc.	alphanumeric string
Mailing Address City		alphanumeric string

Feedback or Questions to: **dtackett@wvsos.gov**

AMERICAN OVERSIGHT



Voter Data Share Cooperative

Field Name	Description or Additional Detail	Likely or Suggested Format
Mailing Address State		char (2)
Mailing Address Zip		numeric (5)
Mailing Address Zip+4		numeric (4)
Phone Number		numeric (123-456-7890)
Email	*user@domain.ext*	alphanumeric string
Drivers License or State Issued ID		alphanumeric string
DL or ID Issuing State		char (2)
SSN 9	Full Social Security Number	numeric (123-45-6789)
SSN Last 4	Last 4 Digits of Social Security Number	numeric (4)
Date of Comparison Vote	Date the Voter cast the ballot for a **double-vote comparison**	Date (YYYY-MM-DD)
Voting Method for Comparison Vote	Election Day/Early/Absentee/Etc.	alphanumeric string
Date of Last Vote	Date the Voter last cast a ballot in **any** election	Date (YYYY-MM-DD)
Challenged / Provisional	Was the vote challenged or considered provisional?	char (Y or N)
Counted	Was the vote counted?	char (Y or N)
Election Date	Date value for **any** election	Date (YYYY-MM-DD)

Feedback or Questions to: **dtackett@wvsos.gov**

AMERICAN OVERSIGHT

From: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
CC: Burns, Kimberly <kburns@OhioSOS.Gov>
Date: 6/12/2023 9:18:25 AM
Subject: RE: Subcommittee and Working Group Updates

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good morning all,

I hope you had a good weekend. Please send your agency's cybersecurity point of contact so that we can start communications with them regarding the secure transfer, retention, and destruction of data.

Thanks,
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

From: Grandjean, Amanda
Sent: Monday, June 5, 2023 3:15 PM
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Subject: Subcommittee and Working Group Updates

Good afternoon all,

I hope you had a great weekend. We had several very productive meetings last week. Thank you to all that actively participated in moving the goal forward. Below is a summary of the meetings last week:

Data Sharing Specifications Subcommittee Meeting Update

On Thursday, June 1, 2023, the Data Sharing Specifications Subcommittee met to discuss the survey that Dave Tackett put together and presented to the group. It was a great conversation that led to several additions to and refinements of the survey. The survey will be used to collect relevant information from each state. This survey will be used to continue to develop the template MOU more comprehensively. Dave will circulate a draft of the survey to the group when it is in a good place to do so. Thanks, Dave, for your leadership! Please let Dave know ASAP if you have any additions to the survey.

We also decided that there needs to be a dedicated group of CISOs/cybersecurity professionals from our offices connected via email to discuss the secure data sharing requirements. **Please respond to this email with your office's cybersecurity point of contact's information** so that we can get this work started on a parallel track to the rest of the work that we are all doing.

Legal MOU Subcommittee Update

The Legal MOU Subcommittee did not meet last week. I don't know about you, but I certainly don't want to have a meeting just for the sake of having a meeting. I've received comments from only about two states now on the template MOU. If you have additional MOUs that you can share with the group or comments to the attached draft template

AMERICAN OVERSIGHT

MOU, please let us know asap. We will continue to plug in data specification language as the Data Sharing Specification Subcommittee builds out the requirements.

Working Group Update

On Friday, June 2, 2023, the Data Sharing Working Group met to discuss subcommittee updates, provide state to state updates, and strategize about next steps. High level notes are set forth below:

- Texas let us know that their legislature passed a bill that would require them to leave ERIC.
- West Virginia discussed conversations they are having with their office of vital statistics regarding death record data. For anyone who is interested, I am happy to provide you with more information regarding how we utilize STEVE data in Ohio.
- Virginia let the group know that they are actively working with their neighboring states to enter into agreements.
- We also discussed leveraging data from our BMVs/DMVs that receive licensure cancellation data from other states to identifying cross-state movers.
- There was discussion about potentially getting NCOA data from the BMV/DMV. If any state is already doing this, please let the group know.
- The group discussed the Limited Access Death Master File Download ("LADMF"). Attached are the instructions and certification documents regarding how to become a certified recipient. You can also access themhere. South Carolina mentioned that they have access to this data via their state data center.
- We also discussed NCOA vendors. Tennessee noted that they have used Melissa Data for NCOA and that Melissa Data also has access to death records from the social security administration.
- Alabama mentioned that they are utilizing a vendor to help them become a certified recipient of this data.
- Ohio continues to have conversations with vendors in the private sector including IBM. We also learned about Thomas Reuters Clear. We can discuss this at our meeting later this week (Friday, June 9, 2023 at 10 a.m. EST).

Please let me know if I missed any notes! Additionally, if you have any questions, please feel free to give me a call.

Thanks!
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

AMERICAN OVERSIGHT

From: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Date: 6/5/2023 2:21:47 PM
Subject: RE: Subcommittee and Working Group Updates

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good afternoon,

Apologies, I had to move the meeting to Thursday, June 8 at 3 p.m. You all should have received a calendar invitation.

Thanks!
Mandi

From: Grandjean, Amanda
Sent: Monday, June 5, 2023 3:15 PM
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Subject: Subcommittee and Working Group Updates

Good afternoon all,

I hope you had a great weekend. We had several very productive meetings last week. Thank you to all that actively participated in moving the goal forward. Below is a summary of the meetings last week:

Data Sharing Specifications Subcommittee Meeting Update

On Thursday, June 1, 2023, the Data Sharing Specifications Subcommittee met to discuss the survey that Dave Tackett put together and presented to the group. It was a great conversation that led to several additions to and refinements of the survey. The survey will be used to collect relevant information from each state. This survey will be used to continue to develop the template MOU more comprehensively. Dave will circulate a draft of the survey to the group when it is in a good place to do so. Thanks, Dave, for your leadership! Please let Dave know ASAP if you have any additions to the survey.

We also decided that there needs to be a dedicated group of CISOs/cybersecurity professionals from our offices connected via email to discuss the secure data sharing requirements. **Please respond to this email with your office's cybersecurity point of contact's information** so that we can get this work started on a parallel track to the rest of the work that we are all doing.

Legal MOU Subcommittee Update

The Legal MOU Subcommittee did not meet last week. I don't know about you, but I certainly don't want to have a meeting just for the sake of having a meeting. I've received comments from only about two states now on the template MOU. If you have additional MOUs that you can share with the group or comments to the reattached draft template MOU, please let us know asap. We will continue to plug in data specification language as the Data Sharing Specification Subcommittee builds out the requirements.

Working Group Update

On Friday, June 2, 2023, the Data Sharing Working Group met to discuss subcommittee updates, provide state to state updates, and strategize about next steps. High level notes are set forth below:

- Texas let us know that their legislature passed a bill that would require them to leave ERIC.
- West Virginia discussed conversations they are having with their office of vital statistics regarding death record data. For anyone who is interested, I am happy to provide you with more information regarding how we utilize STEVE data in Ohio.
- Virginia let the group know that they are actively working with their neighboring states to enter into agreements.
- We also discussed leveraging data from our BMVs/DMVs that receive licensure cancellation data from other states

AMERICAN OVERSIGHT

- to identifying cross-state movers.
- There was discussion about potentially getting NCOA data from the BMV/DMV. If any state is already doing this, please let the group know.
- The group discussed the Limited Access Death Master File Download ("LADMF"). Attached are the instructions and certification documents regarding how to become a certified recipient. You can also access themhere. South Carolina mentioned that they have access to this data via their state data center.
- We also discussed NCOA vendors. Tennessee noted that they have used Melissa Data for NCOA and that Melissa Data also has access to death records from the social security administration.
- Alabama mentioned that they are utilizing a vendor to help them become a certified recipient of this data.
- Ohio continues to have conversations with vendors in the private sector including IBM. We also learned about Thomas Reuters Clear. We can discuss this at our meeting later this week (Friday, June 9, 2023 at 10 a.m. EST).

Please let me know if I missed any notes! Additionally, if you have any questions, please feel free to give me a call.

Thanks!
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

AMERICAN OVERSIGHT

From: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Date: 6/5/2023 2:15:22 PM
Subject: Subcommittee and Working Group Updates
Attachments: State to State Data Sharing MOU 4-27-23 DRAFT.docx
0692-0015 LADMF_ACAB Application Form for Firewalled Status OMB Approved 03-31-2020 Sample.pdf
NTIS LADMF State or Local Government Auditor General or Inspector General Systems Safeguards Att.pdf
LADMF Non-Federal Subscriber Agreement Form_SAMPLE.pdf
NTIS LADMF Accredited Conformity Assessment Body Systems Safeguards Attestation Form_SAMPLE.pdf
LADMF Non-federal Licensee Agreement Form for Use and Resale_SAMPLE.pdf
0692-0013 Limited Access Death Master File Certification Form OMB Approved 03-31-2020 Sample.pdf

---

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good afternoon all,

I hope you had a great weekend. We had several very productive meetings last week. Thank you to all that actively participated in moving the goal forward. Below is a summary of the meetings last week:

Data Sharing Specifications Subcommittee Meeting Update

On Thursday, June 1, 2023, the Data Sharing Specifications Subcommittee met to discuss the survey that Dave Tackett put together and presented to the group. It was a great conversation that led to several additions to and refinements of the survey. The survey will be used to collect relevant information from each state. This survey will be used to continue to develop the template MOU more comprehensively. Dave will circulate a draft of the survey to the group when it is in a good place to do so. Thanks, Dave, for your leadership! Please let Dave know ASAP if you have any additions to the survey.

We also decided that there needs to be a dedicated group of CISOs/cybersecurity professionals from our offices connected via email to discuss the secure data sharing requirements. **Please respond to this email with your office's cybersecurity point of contact's information** so that we can get this work started on a parallel track to the rest of the work that we are all doing.

Legal MOU Subcommittee Update

The Legal MOU Subcommittee did not meet last week. I don't know about you, but I certainly don't want to have a meeting just for the sake of having a meeting. I've received comments from only about two states now on the template MOU. If you have additional MOUs that you can share with the group or comments to the reattached draft template MOU, please let us know asap. We will continue to plug in data specification language as the Data Sharing Specification Subcommittee builds out the requirements.

Working Group Update

On Friday, June 2, 2023, the Data Sharing Working Group met to discuss subcommittee updates, provide state to state updates, and strategize about next steps. High level notes are set forth below:

- Texas let us know that their legislature passed a bill that would require them to leave ERIC.
- West Virginia discussed conversations they are having with their office of vital statistics regarding death record data. For anyone who is interested, I am happy to provide you with more information regarding how we utilize STEVE data in Ohio.
- Virginia let the group know that they are actively working with their neighboring states to enter into agreements.
- We also discussed leveraging data from our BMVs/DMVs that receive licensure cancellation data from other states

AMERICAN OVERSIGHT

- to identifying cross-state movers.
- There was discussion about potentially getting NCOA data from the BMV/DMV. If any state is already doing this, please let the group know.
- The group discussed the Limited Access Death Master File Download ("LADMF"). Attached are the instructions and certification documents regarding how to become a certified recipient. You can also access themhere. South Carolina mentioned that they have access to this data via their state data center.
- We also discussed NCOA vendors. Tennessee noted that they have used Melissa Data for NCOA and that Melissa Data also has access to death records from the social security administration.
- Alabama mentioned that they are utilizing a vendor to help them become a certified recipient of this data.
- Ohio continues to have conversations with vendors in the private sector including IBM. We also learned about Thomas Reuters Clear. We can discuss this at our meeting later this week (Friday, June 9, 2023 at 10 a.m. EST).

Please let me know if I missed any notes! Additionally, if you have any questions, please feel free to give me a call.

Thanks!
Mandi

Amanda M. Grandjean, Esq. | Senior Advisor to the Secretary and Deputy Assistant Secretary of State
Office of the Ohio Secretary of State

O: 614.466.3899
C: 330.412.4467
OhioSoS.gov

AMERICAN OVERSIGHT

MEMORANDUM OF UNDERSTANDING

For Interstate Voter Registration Data Comparison

May, 2023

THIS MEMORANDUM OF UNDERSTANDING ("MOU") is made between the chief state election officials respectively of the States of Ohio, (State), (State), and (State) (Collectively "The States").

Purpose:

WHEREAS, the States recognize the importance of preventing voting fraud and of preserving the integrity of the electoral process;

WHEREAS, the States through the offices of the chief state election officials and under the authority of the respective state laws have each separately implemented a centralized, interactive, computerized statewide voter registration list;

WHEREAS, the existence of centralized, interactive, computerized statewide voter registration lists facilitates the interoperability of such lists for the purpose of comparing voter registration data;

WHEREAS, the States acknowledge that the sharing of voter registration data is a critical tool in detecting and preventing voter fraud;

WHEREAS, the States desire to enter into this Memorandum of Understanding to set the terms of an agreement on behalf of their respective offices to share certain voter registration data amongst themselves for the purposes of investigating and preventing voter fraud;

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties do hereby agree as follows:

I. Legal Authority

This Memorandum of Understanding ("MOU") is being entered into accordance with:

1. Public Law 107-252, the Help America Vote Act of 2002, which required a variety of changes to election processes, among those changes being the implementation of a centralized, interactive, computerized statewide voter list.

2. 52 U.S.C. 20504(d) which states that "[any] change of address form submitted in accordance with State law for purposes of a State motor vehicle driver's license shall serve as notification of change of address for voter registration with respect to elections for Federal office for the registrant involved unless the registrant states on the form that the change of address is not for voter registration purposes."

3. 18 U.S.C. 2721-2725 (federal Driver's Privacy Protection Act (DPPAs) which prohibit bureaus of motor vehicles (BMVs) from disclosing or making available to any person or entity any personal information about an individual that the BMVs obtained in connection with a motor vehicle record unless the person or entity qualifies for that information under one of the

DRAFT

AMERICAN OVERSIGHT

enumerated exceptions to the DPPAs. The parties agree that, for purposes of this MOU, the chief election officer of each state qualifies as a "government agency carrying out its functions" pursuant to the exceptions contained in 18 U.S.C. 2721(b)(1) and (a)(2), or any other analogous state statute, and therefore, may lawfully receive "personal information" and "highly sensitive personal information" as those terms are defined in 18 U.S.C. 2725(3) and (4).

4. Ohio Revised Code 3503.15, which authorizes the Secretary of State to provide such otherwise confidential information or data to persons or organizations that are engaging in legitimate governmental purposes related to the maintenance of the statewide voter registration database.

5. Ohio Administrative Code 111:3-4 which authorizes the Secretary of State to enter into agreements with persons or organizations engaging in legitimate governmental purposes to share information or data as necessary for maintenance of the statewide voter registration database, including election officials of other states, territories, or local political subdivisions of other states or territories who administer elections, for the purpose of comparing voter registration records to assist in identifying duplicate registrations and confirming accurate voter registration information.

Commented [SJ1]: Some states mentioned that they can only share data with an NGO

6. Ohio Revised Code Chapter 3599 which sets forth penalties for criminal voting offenses including but not limited to False voter registration, Illegal voting, and Impersonating another to obtain an absent voter's ballot.

7. [Area for other states' statutes/rules]

II. State Responsibilities

States hereby agree as follows:

1. States agree to share voter registration information for the purpose of confirming accurate voter registration information, including identifying duplicate registrations and instances of multiple votes by the same individuals.

2. Upon written request from a State ("Requesting State"), States shall promptly transmit the following data ("State Data") to the office of the chief election officer of the Requesting State:

    a. All inactive and active voter files (including those records that are confidential or protected from public disclosure by law), including the following fields pursuant to Section III, Data Transmission and Privacy:

Commented [SJ2]: Similar to above comment. Do other states' laws allow this?

        i. 1. All name fields
        ii. 2. All address fields
        iii. 3. Driver's license or state ID number
        iv. 4. Last four digits of Social Security number
        v. 5. Date of birth
        vi. 6. Activity dates, including voting history
        vii. 7. Current record status
        viii. 8. Phone number
        ix. 9. E-mail address or other electronic contact method

DRAFT

AMERICAN OVERSIGHT

b. All licensing or identification records from motor vehicle departments (excluding those fields unrelated to voter eligibility, such as fields related to an individual's driving record), including the fields identified in (2)(a) of this section ("MVD Data").

3. The Requesting State will perform a data comparison by reviewing their own State Data with the requested State Data in order to detect potential voter fraud.

4. The Requesting State will return the results of the data comparison ("Match Results") to the State from which it requested data. The data will include the State possessing the matching record, any additional information about such voter provided by that State, and the date the voter registered in said State.

5. The Match Results by the requesting State shall also include any of the following:

a. Any individual who has voting history but does not appear to be registered to vote
b. Any individual who appears to have moved from one State to another.
c. Duplicate voter registrations.
d. Voters who have appeared to have voted more than once in the same election.
e. Voters who have appeared to have voted in multiple jurisdictions in the same election.
f. Voters who have appeared to have voted on behalf of a deceased voter.
g. Voters who may have died.

6. All data will be transferred between States using the methods and technologies listed in Section III, Data Transmission and Privacy.

7. States agree to share State Data every six months commencing from the Effective Date of this Agreement. States may share data sooner than the stipulated period by providing written notice to each other. Any such early sharing of data will be subject to mutual agreement on the format, content, and timing of the data shared.

8. States additionally agree to share State Data within ninety (90) days following federal general elections occurring during even-numbered years.

9. Each chief state election official shall designate such staff from their respective office as may be deemed necessary to carry out the terms of the Memorandum of Understanding.

Commented [SJ3]: Discuss generally

Commented [SJ4]: What do we want this to cover? What will actually need to be sent over? On the call it was noted we don't want to just send lists of everyone that may have died.

Commented [SJ5]: Discuss

Commented [SJ6]: Changed from 30 based off feedback from call

Commented [SJ7]: Clarified based off feedback from call

III. Data Transmission and Privacy

TBD

IV. Records Requests and Confidentiality

1. When a State receives a Records Request for State Data or Match Results ("The Responding State"), and it reasonably appears that such request may capture State Data obtained from a different State ("The Subject State"), the Receiving State shall promptly notify the Subject State in writing of the request and the data sought. All requests shall be governed by the Responding State's public records law in addition to any applicable federal statute. The Responding State

Commented [SJ8]: To discuss. What are the ramifications of differences between public records statutes? (i.e. a record may be exempt in one state but not another)

DRAFT

AMERICAN OVERSIGHT

shall provide written notice to the Subject State regarding any legal determination and response to the Records Request.

2. States represent and warrant that the transmission of State Data and Match Results shall be conducted in compliance with applicable state, federal, and local laws, rules and regulations. A State shall not have an obligation under this Agreement to release State Data or Match Results in response to a Records Request even if authorized to so under this Agreement, including, by way of example and not limitation, if the State determines that doing so would violate an applicable law in that State's jurisdiction.

3. States shall not use, transmit, sell, or disclose Match Results from another State or any State Data for any purpose other than supporting the function of this Memorandum and responding to lawful public records requests.

4. States agree that they shall protect and prohibit disclosure of State Data and Match Results pursuant to any applicable state or federal law.

5. Should there be an unauthorized or impermissible disclosure or transmission of State Data or Match Results, regardless of whether it is accidental or intentional ("Unauthorized Disclosure"), the State that disclosed or transmitted the Match Results or State Data shall take the following steps:

    a. Notice to States: The State that disclosed or transmitted the State Data shall immediately notify any other State whose State Data was included in the disclosure or transmission.
    b. Where applicable, the State that disclosed or transmitted the State Data shall address the Unauthorized Disclosure with law and keep other States whose State Data was included in the Unauthorized Disclosure reasonably apprised of its efforts to do so.
    c. Within ninety (90) days of an Unauthorized Disclosure, the State which disclosed or transmitted the State Data shall explain in writing that such Unauthorized Disclosure has been cured and how it was cured or, if the breach is not curable, provide a written explanation of what steps it has taken to mitigate the risks to other States resulting from such breach.

6. States agree that the federal statutes and regulations identified below ("Federal Protections") protect and prohibit the disclosure of certain State Data and/or Match Results. The States agree to prevent disclosure of and otherwise protect State Data and Match Results in accordance with the Federal Protections including when responding to a Records Request.

    a. Driver's Privacy Protection Act ("DPAA"): State Data and Match Results are protected from disclosure under the DPPA, 18 U.S.C. § 2721, *et seq*, unless a statutory exception applies.

    b. LADMF Regulations- Add later?

    c. NCOALink Regulations- Add Later?

Commented [SJ9]: To discuss

V. Term of this MOU; Removal and Resignation

1. This MOU is effective upon signature of State and shall remain in effect, unless it is amended or

DRAFT

AMERICAN OVERSIGHT

rescinded, until January 1, 2027.

2. Any State that is a party to this MOU may terminate their agreement upon providing written notice of their intent to terminate at least thirty (30) days prior to the desired termination date. Upon such termination, the State shall be relieved of all further obligations and liabilities under this MOU.

3. Any State that terminates their agreement [Terminating State] shall delete all State Data and Match Results that did not originate within the Terminating State within fourteen (14) days or at the earliest possible time pursuant to that State's public records law, whichever is sooner.

VI. Amendments

1. Any State that is a party to this MOU may propose amendments to this agreement by providing written notice to all other States. Such notice shall describe the proposed amendment in detail. The proposed amendment shall be deemed accepted and incorporated into this MOU if all other States agree to it in writing.

VII. State Representations

1. State represents and warrants that the transmission of State Data and Match Results to other States required under this Agreement is and shall continue to be conducted in compliance with applicable state, federal, and local laws, rules and regulations.

2. States shall not use, transmit, or disclose any State Data or Match Results for any purpose other than the administration of elections under state or federal law, supporting the operations of this Agreement, and responding to Records Requests consistent with the terms of this Agreement.

3. Member shall use its best efforts to prevent the Unauthorized Disclosure (defined in Section IV of this Agreement) of State Data, Match Results, or other protected State information.

VIII. Miscellaneous

1. Waiver. No waiver by any party for any breach by the other of any of the provisions of this Agreement shall be deemed a waiver of any preceding or succeeding breach of the same or any other provisions hereof. No such waiver shall be effective unless in writing and then only to the extent expressly set forth in writing.

2. Severability. The provisions of this Agreement are separate and severable, and the invalidity of any of them shall not affect or impair the validity or enforcement of the remaining provisions.

3. Assignment. Member States may not sell, assign, or otherwise transfer any rights or interests or delegate any duties or obligations in this MOU, without approval of a majority of Member States.

4. Complete Agreement. This Agreement is the parties' final and binding expression of their agreement and the complete and exclusive statement of its terms. This MOU cancels, supersedes and revokes all prior negotiations, representations and agreements between the States, whether oral or written, relating to the subject matter of this MOU.

DRAFT

AMERICAN OVERSIGHT

5. Headings and Subsections. Section headings are provided for reference and do not constitute part of this MOU.

IX. Notices

1. All notices permitted or required hereunder shall be in writing and shall be transmitted either: via certified or registered United States mail, return receipt requested; by facsimile transmission; by personal delivery; by expedited delivery service; or by e-mail with acknowledgement of receipt of the notice.
2. Such notices shall be addressed as follows or to such different addresses as the Parties may from time-to-time designate:

State
Name:
Title:
Address:
Phone:
E-Mail:

State
Name:
Title:
Address:
Phone:
E-Mail:

STATE	**STATE**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

DRAFT

AMERICAN OVERSIGHT

Limited Access Death Master File
Accredited Conformity Assessment Body
Application Form for Firewalled Status

This form is required ONLY for an Accredited Conformity Assessment Body (ACAB) owned, managed, or controlled by the Person or Certified Person, as defined in 15 CFR 1110.2, that it is assessing for access to the Limited Access Death Master File (LADMF).

1. The undersigned hereby represents and warrants that he or she is authorized to make this certification on behalf of, and to bind, the ACAB applying for firewalled status pursuant to 15 CFR 1110. 502.

2. The undersigned certifies that the ACAB is "owned, managed or controlled," as that term is defined in 15 CFR 1110.501, by the following Person or Certified Person:

   Enter Legal Name of Person or Certified Person:

3. The undersigned further certifies that assessment or audit by the ACAB would provide equal or greater assurance that the Person or Certified Person has information security systems, facilities, and procedures in place to protect the security of the LADMF than would the Person's or Certified Person's use of an independent third party conformity assessment body as required by 15 CFR 1110.502(b)(1).

4. In making the certification in paragraph 3., the undersigned states that the ACAB makes this assurance based upon the following facts:

   Explain the basis for assurances:

5. The undersigned further certifies that the ACAB has established procedures to ensure that, as required by 15 CFR 1110.502(b)(2):
   (i) Its attestations and audits are protected from undue influence by the Person or Certified Person that is the subject of attestation or audit by the organization, or by any other interested party;
   (ii) NTIS will be notified promptly of any attempt by the Person or Certified Person that is the subject of attestation or audit by the organization, or by any other interested party, to hide or exert undue influence over an attestation or audit; and
   (iii) Allegations of undue influence may be reported confidentially to NTIS.

6. In making the certification in paragraph 5., the undersigned states that the ACAB makes these representations based upon the following facts:

   Explain the procedures:

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000629

7. The undersigned agrees that the ACAB will cooperate in response to any request from NTIS to verify the accuracy, veracity and/or completeness of the information received in connection with this application for firewalled status.

8. The undersigned hereby declares that all certifications and statements made herein are true to the best of his or her knowledge and belief, and further that these certifications and statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment of not more than five (5) years, or both, under 18 U.S.C. Section 1001.

Signature: _____

Name: _____

Corporate Name: _____

Address: _____

_____

Phone Number: _____

Email: _____

_____

Date: _____

Fax to 703-605-6900
National Technical Information Service
U.S. Department of Commerce
5301 Shawnee Rd.
Alexandria, VA 22312

SAMPLE

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information.

Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Technical Information Service, Attn: Daniel Ramsey, National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312; dramsey@ntis.gov, (703-605-6703).

OMB Control: 0692-0015
Expiration date: 03/31/2023
NTIS FM101

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000030

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

LIMITED ACCESS DEATH MASTER FILE (LADMF) STATE OR LOCAL GOVERNMENT AUDITOR GENERAL (AG) OR INSPECTOR GENERAL (IG) SYSTEMS SAFEGUARDS ATTESTATION FORM

TO BE COMPLETED BY A STATE OR LOCAL GOVERNMENT AUDITOR GENERAL OR INSPECTOR GENERAL.

NTIS FM 100B | REVISION 0.2 | DATED 11 OCTOBER 2016

FORM INSTRUCTIONS FOR STATE AND LOCAL GOVERNMENT APPLICANTS

PRIOR TO BEING GRANTED ACCESS TO LADMF DATA AND PRODUCTS FROM NTIS, ANY STATE OR LOCAL GOVERNMENT DEPARTMENT OR AGENCY RELYING ON AN ATTESTATION FROM A STATE OR LOCAL AG OR IG IS **REQUIRED** TO HAVE THIS FULLY COMPLETED FORM SUBMITTED BY THE AG OR IG.

1. Review the requirements for accessing and using LADMF data and products at https://dmf.ntis.gov.
2. The state or local AG or IG completes this form for a specific person* applying for LADMF certification.
3. The state or local AG or IG submits this completed form directly to NTIS. NTIS will not accept Form NTIS FM100B directly from an applicant.

SECTION 1: STATE OR LOCAL GOVERNMENT APPLICANT INFORMATION

NAME OF APPLICANT STATE OR LOCAL GOVERNMENT DEPARTMENT OR AGENCY

NTIS INVOICE/ORDER CONFIRMATION NUMBER FOR PROCESSING FEE:

**Per 15 CFR Part 1110, a "person" includes a corporation, company, association, firm, partnership, society, joint stock company, other private organization, or state or local government department or agency, or individual.*

SECTION 2: STATE OR LOCAL **GOVERNMENT** AUDITOR GENERAL OR INSPECTOR GENERAL

NAME OF ASSESSOR	E-MAIL OF ASSESSOR
AG/IG OFFICE	PHONE NUMBER

SECTION 3: ASSESSMENT RESULTS

An assessment of the state or local government applicant named in Section 1 was completed and based on the findings the applicant has systems, facilities and procedures in place to safeguard LADMF information as required by 15 CFR 1110.102(a)(2). This assessment was conducted on _____ [enter date of assessment], which is no more than 3 years prior to the date of the applicant's completed Form NTIS FM 161.

If this assessment was not conducted specifically or solely for the purpose of submission under 15 CFR Part 1110, describe below the nature of the assessment upon which the assessment result in this Section 3 is based (note if additional documentation is being submitted):

SAMPLE

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

LIMITED ACCESS DEATH MASTER FILE (LADMF) CERTIFICATION FOR STATE OR LOCAL GOVERNMENT AUDITOR GENERAL (AG) OR INSPECTOR GENERAL (IG)

SYSTEMS SAFEGUARDS ATTESTATION FORM

TO BE COMPLETED BY A STATE OR LOCAL GOVERNMENT AUDITOR GENERAL OR INSPECTOR GENERAL.

NTIS FM 100B | REVISION 0.2 | DATED 11 OCTOBER 2016

SECTION 4: STATE **OR** LOCAL GOVERNMENT **AG OR IG** A**TTESTATION**

The undersigned State or Local Auditor General or Inspector General hereby attests that:

1. It has read and understands the regulations in 15 CFR Part 1110.

2. It will cooperate in response to any request from NTIS to verify the accuracy, veracity, and/or completeness of information received in connection with its assessment and this attestation.

By signing and submitting this form I attest that I am authorized to sign this form on behalf of the State or Local Government AG or IG identified in Section 2, that the State or Local Government AG or IG identified in Section 2 has conducted a full assessment of the LADMF systems safeguards program of the applicant identified in Section 1, and that the results are as specified in Section 3. I hereby acknowledge that any willful false attestation or statement made herein is punishable under 18 U.S.C. §1001 by fine or imprisonment of not more than five (5) years, or both.

Signature: _____

Date: _____

Email to: DMFCERT@NTIS.GOV Fax to: 703.605.6900

SAMPLE

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 3 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Technical Information Service, Attn: Daniel Ramsey, National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312; dramsey@ntis.gov, (703-605-6703).

OMB Control No.:
0692-0016 Expiration Date:
10/31/2023

AMERICAN OVERSIGHT

U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

Agreement No. _____

Limited Access Death Master File Non-Federal Subscriber Agreement

The Agreement is entered into between the National Technical Information Service (NTIS), U.S. Department of Commerce and [Enter Subscriber's Name], hereinafter referred to as "Subscriber."

1. Scope: If Subscriber does not have a current Death Master File (DMF) subscription in place with NTIS, Subscriber agrees to transfer to NTIS funding consistent with the attached Limited Access Death Master File Subscriber Order Form (Attachment A1) or Limited Access Death Master File: Online Search Price List and Order Form (Attachment A2). In consideration of such payment, NTIS agrees to provide Subscriber with the Limited Access DMF, as defined in 15 CFR § 1110.2. NTIS also grants to Subscriber a non-exclusive, non-transferable right to make the Limited Access DMF available only to Subscriber's employees, contractors, and subcontractors whom Subscriber has determined meet the requirements to be a Certified Person as set forth in regulations found at 15 CFR § 1110.2.

2. Authority: NTIS is authorized to enter into this Agreement and receive funds under 15 U.S.C. §§ 1153 and 3704b note. NTIS is authorized to perform the services detailed in this Agreement, including providing the Limited Access DMF to Subscriber, pursuant to 15 U.S.C. § 3704b and 15 U.S.C. §§ 1151-1157. In addition, NTIS is authorized to establish a certification program under which persons may obtain immediate access to the Death Master File (DMF), pursuant to § 203 of the Bipartisan Budget Act of 2013.

3. Requirements for Subscribers:

(a) Subscriber must at all times during this Agreement be a Certified Person as defined in 15 CFR §1110.2.

(b) Subscriber agrees that beginning on the effective date of this Agreement, all provisions of this Agreement apply to any and all Limited Access DMF provided to Subscriber by NTIS under this Agreement.

(c) Should any of the information to which it certified on the Subscriber Certification Form change during the term of this Agreement, Subscriber agrees to notify NTIS of the change and whether Subscriber believes the change results in loss of Subscriber's status as a Certified Person, in writing, immediately, but no later than 24 hours after Subscriber becomes aware of the change.

(d) Should Subscriber cease to be a Certified Person during the term of this Agreement, Subscriber agrees to destroy all Limited Access DMF provided to Subscriber by NTIS under this Agreement and will certify to NTIS in writing that is has destroyed all such Limited Access DMF.

(e) Subscriber agrees that if it uses the DMF on a continuing basis it must, after receiving an updated complete DMF, keep that file updated by continually purchasing and incorporating all regular updates (new deaths/changes/deletions), beginning with the same month as the original file.

(f) Subscriber agrees to be subject to audit by NTIS to determine Subscriber's compliance with the requirements of 15 CFR Part 1110. Subscriber agrees to permit NTIS to conduct periodic and unscheduled audits of the systems, facilities, and procedures of Subscriber relating to Subscriber's safeguards for, access to, and use and distribution of, Limited Access DMF, during regular business hours. Subscriber understands and agrees that failure to cooperate with any NTIS audit may result in immediate termination of this Agreement.

(g) Subscriber agrees to retain a list of all employees, contractors, and subcontractors to which it provides Limited Access DMF and to make that list available to NTIS as part of any audits conducted under paragraph (f) above.

4. Authorized Purposes: The rights granted to Subscriber under this Agreement are solely for Authorized Purposes. Authorized Purposes are limited to search, retrieval, display, downloading and processing of Limited Access DMF by Subscriber and Subscriber's employees, contractors and subcontractors who meet the requirements to be a Certified Person as set forth in 15 CFR 1110.102, through Subscriber's computer system on Subscriber's premises.

SAMPLE

AMERICAN OVERSIGHT

U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

Agreement No. _____

Limited Access Death Master File
Non-Federal Subscriber Agreement

5. Prohibited Purposes: Sale or redistribution of Limited Access DMF, or copying, modifying, or posting all or a portion of Limited Access DMF for the purpose of modifying it, or posting modified DMF on the public Internet are expressly prohibited under this Agreement. In addition, sublicensing or re-distributing the Limited Access DMF to another party, making it available to other parties via the World Wide Web or other gateway, or to otherwise making it available to users who are not Subscriber's employees, contractors, or subcontractors who meet the requirements to be a Certified Person as set forth in 15 CFR 1110.102, are also prohibited.

6. Security: In order to safeguard the Limited Access DMF provided to Subscriber under this Agreement, Subscriber agrees that:

(a) Subscriber will at all times have security provisions in place to protect the Limited Access DMF from being visible, searchable, harvestable, or in any way discoverable on the World Wide Web. Subscriber represents that it currently has, and will maintain for the term of this Agreement, systems, facilities, and procedures in place to safeguard all Limited Access DMF, and experience in maintaining the confidentiality, security, and appropriate use of Limited Access DMF, pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to Subscriber, and agrees to audits as set forth in this Agreement.

(b) Subscriber understands that any successful attempt by any person to gain unauthorized access to or use of the Limited Access DMF from Subscriber may result in immediate termination of this Agreement. In addition, any successful attempt by any person to gain unauthorized access may under appropriate circumstances result in penalties as prescribed in 15 CFR §1110.200 levied on both Subscriber and the person attempting such access. Any unauthorized access or attempted unauthorized access is a breach or attempted breach of security and must immediately be reported to NTIS at dmfcert@ntis.gov.

7. Payment: If Subscriber does not have a current DMF subscription in place with NTIS, Subscriber agrees to pay applicable fees in advance in accordance with the fee schedules in Attachment A1 or Attachment A2 to this Agreement, as applicable. NTIS reserves the right to change any fees set forth in Attachment A1 or Attachment A2, to establish new fees or to waive fees during the term of this Agreement by giving Subscriber 90 days advance notice.

8. Penalties: Subscriber acknowledges that failure to comply with the provisions of paragraph (3) of the Subscriber Certification Form may subject the Subscriber to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

9. Liability: The U.S. Government/NTIS (a) makes no warranty, express or implied, with respect to information provided under this agreement, including, but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assumes no liability for any direct, indirect or consequential damages flowing from any use of any part of the Limited Access DMF, including infringement of third party intellectual property rights; and (c) assumes no liability for any errors or omissions in Limited Access DMF. Subscriber hereby waives, relinquishes and releases the U.S. Government/NTIS from any claim for damage or injury arising from its acquisition or use of the Limited Access DMF or in any products derived from it.

Without limiting in any way the scope and breadth of the foregoing, the parties acknowledge that the Limited Access DMF has inaccuracies and that NTIS and the Social Security Administration (SSA), which provides the DMF to NTIS, do not guarantee the accuracy of the Limited Access DMF. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the Limited Access DMF is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the Limited Access DMF. (See Attachment B.)

SAMPLE

AUDIT OVERSIGHT

Limited Access Death Master File
Non-Federal Subscriber Agreement

10. Indemnification and Hold Harmless: To the extent not prohibited by law, Subscriber shall indemnify and hold harmless the U.S. Government/NTIS from all claims, liabilities, demands, damages, expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with Subscriber's or Subscriber's employees, contractors, or subcontractors use of the Limited Access DMF. This provision shall survive termination of this Agreement and will include any and all claims or liabilities arising from intellectual property rights.

11. Governing Law: This Agreement will be governed by applicable Federal law.

12. Term of Agreement and Amendments: This agreement is effective on the last date of signature by the parties below and will remain in effect for one year or, if Subscriber has a current DMF subscription in place with NTIS, the subscription expiration date, whichever is earlier. This Agreement may be renewed on an annual basis by written amendments signed by both parties for up to five years, contingent upon Subscriber executing the current version of the Subscriber Certification Form annually and fulfilling any and all other requirements set forth in NTIS regulations found at 15 CFR part 1110. This Agreement may be amended at any time by a written amendment signed by both parties. Subscriber must be a Certified Person throughout the term of this Agreement, and subscription will be immediately terminated if Subscriber loses status as a Certified Person.

13. Termination: Either party may terminate the Agreement by giving the other 90 days written notice. If Licensee terminates, Licensee will not receive any refund, proration or abatement of any fees paid to NTIS. If NTIS terminates, Licensee will receive a refund for the unused portion of the Annual Fee unless Licensee is in breach of this Agreement, or has violated 15 CFR part 1110, in either case as determined by NTIS. Upon termination of this Agreement by either party, Subscriber agrees to destroy all Limited Access DMF provided to Subscriber by NTIS under this Agreement and will certify to NTIS in writing that is has destroyed all such Limited Access DMF.

14. Resolution of Disagreements: Should disagreements arise on the interpretation of the provisions of this Agreement or amendments and/or revisions thereto, that cannot be resolved at the operating level, the area(s) of disagreement shall be stated in writing by each party and presented to the other party for consideration. If agreement or interpretation is not reached within 30 days, the parties shall forward the written presentation of the disagreement to respective higher officials for appropriate resolution.

Both parties agree that all claims, disputes, and/or causes of action arising under or related to this Agreement, not resolved in the dispute resolution process, shall be brought in a court/forum of competent Federal jurisdiction.

SAMPLE

AUDIT OVERSIGHT

Limited Access Death Master File
Non-Federal Subscriber Agreement

15. Contact Information:

A. Program Management:

Subscriber	Primary	Alternate
Contact Name		
Organization		
Address		
Phone Number		
Fax Number		
Email Address		
NTIS	**Primary**	**Alternate**
Contact Name	Daniel Ramsey	
Organization	National Technical Information Service (NTIS); Manager, Office of Product and Program Management	
Address	National Technical Information Service (NTIS) 5301 Shawnee Road Alexandria, Virginia 22312	
Phone Number	703-605-6703	
Fax Number	703-605-6372	
Email Address	dramsey@ntis.gov	

SAMPLE

AUDIT OVERSIGHT

Limited Access Death Master File
Non-Federal Subscriber Agreement

B. Financial:

Subscriber	Primary	Alternate
Contact Name		
Organization		
Address		
Phone Number		
Fax Number		
Email Address		
NTIS	**Primary**	**Alternate**
Contact Name	NTIS Accounting	NTIS Accounting
Organization	NTIS Accounting	NTIS Accounting
Address	5301 Shawnee Road Alexandria, VA 22312	5301 Shawnee Road Alexandria, VA 22312
Phone Number	703-605-6600	703-605-6600
Fax Number	703-605-6743	703-605-6743
Email Address	lharper@ntis.gov	cscott@ntis.gov

SAMPLE

AUDIT OVERSIGHT

SUBSCRIBER:

Authorized Signature

_____

Name: _____

Corporate Name: _____

Address: _____

_____

Phone Number: _____

NTIS Subscription Number: _____

NTIS Certification Invoice/Confirmation Number: _____

_____

Subscription Administrator _____

_____

_____

Date _____

Fax to 703-605-6900
National Technical Information Service
U.S. Department of Commerce
5301 Shawnee Rd.
Alexandria, VA 22312

SAMPLE

Attachment A1: Limited Access Death Master File Subscriber Order Form
Attachment A2: Limited Access Death Master File: Online Search Price List and Order Form
Attachment B: Important Information – Mandatory Requirements Death Master File

LADMF Terms and Conditions Revised 3-24-2014

AMERICAN OVERSIGHT

Attachment B

Important Information-Mandatory Requirements Death Master File

IMPORTANT INFORMATION – MANDATORY REQUIREMENTS
DEATH MASTER FILE

TO ALL SUBSCRIBERS PURCHASING THE SOCIAL SECURITY ADMINISTRATION'S (SSA) DEATH MASTER FILE (DMF):

As a result of a court case under the Freedom of Information Act, SSA is required to release its death information to the public. SSA's DMF contains the complete and official SSA database extract, as well as updates to the full file of persons reported to SSA as being deceased. However, you, as a subscriber/purchaser of SSA's DMF, are advised at the time of initial purchase that the DMF does have inaccuracies and **SSA DOES NOT GUARANTEE THE ACCURACY OF THE DMF FILE.** SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on this file is not proof that the individual is alive. Further, in rare instances it is possible for the records of a person who is not deceased to be included erroneously in the DMF. If an individual seeing your copy of the DMF has a complaint that they find erroneous data/death information on that DMF, you should advise them to follow the procedures listed below. In fact, **you should be providing the information below in your publication, if any,** of the DMF:

ERRORS – If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the DMF), the individual should be told to contact their local Social Security office (with proof) to have the error corrected. The local Social Security office will:

(1) **make the correction to the main NUMIDENT file at SSA and give the individual a verification document of SSA's current records to use to show any company, recipient/purchaser of the DMF that had the error; OR,**

(2) **find that SSA already has the correct information on the main NUMIDENT file and DMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company subscriber/purchaser of the DMF that had the error.**

In the latter case (2 above), the DMF subscriber (you) probably received the incorrect death data sometime prior to the correction of SSA's main records. (The only way you can now get an updated DMF with the correction would be to again purchase the entire DMF file and keep it current with all of the **MONTHLY OR WEEKLY UPDATES** – See MANDATORY REQUIREMENTS below.) You should accept proof from the individual (his/her own records or the verification s/he received from the local Social Security office) and correct your copy of the DMF. You should also notify any organization to which you sold the DMF that this correction needs to be made.

SAMPLE

AMERICAN OVERSIGHT

MANDATORY REQUIREMENTS:

It is mandatory that all subscribers of the DMF intending to use its data on a continuing basis must, after receiving an updated complete **DMF FULL FILE**, keep that file updated by continually purchasing all **MONTHLY OR WEEKLY UPDATES** (NEW DEATHS/CHANGES/DELETIONS), beginning with the same month as the Full File. If you are not meeting SSA's requirements because you are not receiving the **MONTHLY OR WEEKLY UPDATES ON A CONTINUING BASIS** immediately after receiving the **FULL FILE**, then you are **NOT** keeping your DMF up-to-date with SSA's records. Thus, you are working with a DMF with an increased number of unnecessary inaccuracies and possibly adversely affecting an increased number of individuals. **NO ONE IS TO SELL THE DMF WITHOUT REQUIRING CONTINUOUS SUBSCRIBERS TO ADHERE TO THIS MANDATORY REQUIREMENT FOR KEEPING THEIR DMF UP-TO-DATE.**

YOU, AS A DMF SUBSCRIBER, ARE REMINDED THAT YOU SHOULD NOT TAKE ANY ADVERSE ACTION AGAINST ANY INDIVIDUAL WITHOUT FURTHER INVESTIGATION TO VERIFY THE DEATH LISTED.

If you, as a subscriber to SSA's DMF are making available/selling SSA's DMF information to others, you **MUST ALSO PROVIDE THEM WITH A COPY OF THIS NOTICE.**

NOTE: **DO NOT TELL ANYONE TO CONTACT NTIS OR SSA HEADQUARTERS FOR CORRECTIONS! CORRECTIONS MUST BE MADE AT THE LOCAL SOCIAL SECURITY OFFICE SERVICING THE INDIVIDUAL.**

SAMPLE

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000040

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

LIMITED ACCESS DEATH MASTER FILE (LADMF) ACCREDITED CONFORMITY ASSESSMENT BODY SYSTEMS SAFEGUARDS ATTESTATION FORM

TO BE COMPLETED BY AN ACCREDITED CONFORMITY ASSESSEMENT BODY (ACAB).
NTIS FM 100 A | REVISION 0.2 | DATED 11 OCTOBER 2016

FORM INSTRUCTIONS FOR APPLICANTS

PRIOR TO BEING GRANTED ACCESS TO LADMF DATA AND PRODUCTS FROM NTIS, ALL PERSONS ARE **REQUIRED** TO HAVE THIS FULLY COMPLETED FORM SUBMITTED BY AN ACAB. STATE AND LOCAL GOVERNMENT DEPARTMENTS AND AGENCIES RELYING ON ATTESTATIONS FROM STATE OR LOCAL GOVERNMENT AUDITORS GENERAL OR INSPECTORS GENERAL SHOULD USE FORM NTIS FM 100B.

1. Review the requirements for accessing and using LADMF data and products at https://dmf.ntis.gov.
2. Identify an ACAB to assess your LADMF systems safeguards program implementation.
3. The ACAB submits this completed form directly to NTIS. NTIS will not accept Form NTIS FM100A directly from an applicant.

SECTION 1: APPLICANT INFORMATION

NAME OF APPLICANT ORGANIZATION

NTIS INVOICE/ORDER CONFIRMATION NUMBER FOR PROCESSING FEE:

**Per 15 CFR Part 1110, a "person" includes a corporation, company, association, firm, partnership, society, joint stock company, other private organization, or state or local government department or agency, or individual.*

SECTION 2: INDEPENDENT OR FIREWALLED ACAB

NAME OF ASSESSOR	E-MAIL OF ASSESSOR
COMPANY	PHONE NUMBER

SECTION 3: ASSESSMENT RESULTS

An assessment of the applicant named in Section 1 was completed using _____ [fill in applicable standard(s)] and based on the findings the applicant has systems, facilities and procedures in place to safeguard LADMF information as required by 15 CFR 1110.102(a)(2). This assessment was conducted on _____ [enter date of assessment], which is no more than 3 years prior to the date of the applicant's completed Form NTIS FM 161.

If this assessment was not conducted specifically or solely for the purpose of submission under 15 CFR Part 1110, describe below the nature of the assessment upon which the assessment result in this Section 3 is based (note if additional documentation is being submitted):

SAMPLE

AMERICAN OVERSIGHT

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

(LIMITED ACCESS DEATH MASTER FILE (LADMF) CERTIFICATION ACCREDITED CONFORMITY ASSESSMENT BODY SYSTEMS SAFEGUARDS ATTESTATION FORM

TO BE COMPLETED BY AN ACCREDITED CONFORMITY ASSESSEMENT BODY (ACAB).

NTIS FM 100 A | REVISION 0.2 | DATED 11 OCTOBER 2016

SECTION 4: ACAB ATTESTATION

The undersigned Accredited Conformity Assessment Body hereby attests that:

1. It is either:
   - ☐ An independent third party accredited conformity assessment body that is not "owned, managed, or controlled," as defined in 15 CFR §1110.501, by the applicant identified in Section 1, OR
   - ☐ A firewalled accredited conformity assessment body whose LADMF ACAB Application for Firewalled Status has been accepted by NTIS.
2. It has read and understands the regulations in 15 CFR Part 1110.
3. It is accredited to the following nationally or internationally recognized standard(s) for bodies providing audit and assessment of information security management systems (identify standard(s) and accrediting body(ies)):

4. The scope of the accreditation identified above encompasses the information safeguarding and security requirements set forth in 15 CFR Part 1110.
5. It will cooperate in response to any request from NTIS to verify the accuracy, veracity, and/or completeness of information received in connection with its assessment and this attestation.

By signing and submitting this form I attest that I am authorized to sign this form on behalf of the ACAB identified in Section 2, that the ACAB identified in Section 2 has conducted an assessment of the LADMF systems safeguards program of the applicant identified in Section 1, and that the results are as specified in Section 3. I hereby acknowledge that any willful false attestation or statement made herein is punishable under 18 U.S.C. §1001 by fine or imprisonment of not more than five (5) years, or both.

Signature: _____

Date: _____

Email to: DMFCERT@NTIS.GOV Fax to: 703.605.6900

SAMPLE

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 3 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Technical Information Service, Attn: Daniel Ramsey, National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312; dramsey@ntis.gov (703-605-6703).

OMB Control No.: 0692-0016 Expiration Date: 10/31/2023

AMERICAN OVERSIGHT

U.S. Department of Commerce
National Technical Information Service

Agreement No. _____

National Technical Information Service
Limited Access Death Master File
Non-federal Licensee Agreement for Use and Resale

This Agreement is entered into between the National Technical Information Service (NTIS), U.S. Department of Commerce, and [Enter Licensee's Name], hereinafter referred to as "Licensee."

1. **Scope:** For purposes of this Agreement, Licensee is considered a Subscriber and must execute and submit the Certification Form in order to become a Certified Person. If Licensee does not have a current Limited Access Death Master File (LADMF)subscription in place with NTIS, Licensee agrees to pay to NTIS an annual fee, as set forth in Attachments A1 and A2, in consideration for which NTIS agrees to provide Licensee with the Limited Access Death Master File (LADMF), as defined in 15 CFR § 1110.2, for Licensee's use in accordance with the terms of this Agreement. NTIS also grants to Licensee a non-exclusive, non-transferable right to make the Limited Access Death Master File (LADMF) available for use only to Licensee's employees, contractors, subcontractors, and for resale only to customers who are Federal agencies or Persons. Before the Licensee makes the Limited Access Death Master File (LADMF) available to its employees, contractors, subcontractors, or customers who are Persons, Licensee must determine that the Person meets the requirements to be a Certified Person as set forth in regulations found at 15 CFR § 1110.102.

2. **Authority:** NTIS is authorized to enter into this Agreement and receive funds under 15 U.S.C. §§ 1153 and 3704b note. NTIS is authorized to perform the services detailed in this Agreement, including providing the Limited Access Death Master File (LADMF) to Licensee, pursuant to 15 U.S.C. § 3704b and 15 U.S.C. §§ 1151-1157. In addition, NTIS is authorized to establish a certification program under which persons may obtain immediate access to the Limited Access Death Master File (LADMF), pursuant to § 203 of the Bipartisan Budget Act of 2013.

3. Requirements for Licensees:

(a) Licensee must at all times during this Agreement be a Certified Person as defined in 15 CFR 1110.2.

(b) Licensee agrees that beginning on the effective date of this Agreement, all provisions of this Agreement apply to any and all Limited Access Death Master File (LADMF) provided to Licensee by NTIS under this Agreement.

(c) Should any of the information to which it certified on the Certification Form change during the term of this Agreement, Licensee agrees to notify NTIS of the change and whether Licensee believes the change results in loss of Licensee's status as a Certified Person, in writing, immediately, but in no event later than 24 hours after Licensee becomes aware of the change.

(d) Should Licensee cease to be a Certified Person during the term of this Agreement, Licensee agrees to destroy all Limited Access Death Master File (LADMF) provided to NTIS under this Agreement and will certify to NTIS in writing that is has destroyed all such DMF.

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000043

(e) Licensee must include in all contracts and agreements with others under which Licensee will give access to the Limited Access Death Master File (LADMF), provisions that require the recipients of the Limited Access Death Master File (LADMF) who are Persons (Recipients) to comply with the terms of this Agreement and the requirements of 15 CFR Part 1110, and that require the Recipients to flow down those provisions in any subsequent contracts or other agreements of Recipients for access to the Limited Access Death Master File (LADMF);

(f) Licensee agrees that if it uses the LADMF on a continuing basis it must, after receiving an updated complete LADMF, keep that file updated by continually purchasing and incorporating all regular updates (new deaths/changes/deletions), beginning with the same month as the original file.

(g) Licensee agrees to be subject to audit by NTIS to determine Licensee's compliance with the requirements of 15 CFR Part 1110. Licensee agrees that NTIS may conduct periodic and unscheduled audits of the systems, facilities, and procedures of Licensee relating to Licensee's safeguards for, access to, and use and distribution of, Limited Access Death Master File (LADMF), during regular business hours. Licensee understands and agrees that failure to cooperate with any NTIS audit may result in immediate termination of this Agreement.

(h) Licensee agrees to retain a list of all employees, contractors, subcontractors, and customers to which it provides Limited Access Death Master File (LADMF) and to make that list available to NTIS as part of any audits conducted under paragraph (g) above.

4. **Authorized Purposes:** The rights granted to Licensee under this Agreement are solely for Authorized Purposes. Authorized Purposes are:

(a) Internal Use: Licensee may allow employees of the Licensee organization to search, retrieve, display, download and process data from the Limited Access Death Master File (LADMF) through Licensee's or Licensee's contractors' or partners' computer system for the Licensee organization's own internal needs;

(b) Access: Licensee may combine or integrate the Limited Access Death Master File (LADMF) with other software or technology that Licensee owns or is authorized to use in order to make it easier for Licensee's customers to search the Limited Access Death Master File (LADMF) and retrieve information from it;

(c) Customized Information Products: Licensee may derive information from the Limited Access Death Master File (LADMF) and make that information available to its customers. To obtain such information, customers who are Persons must meet the requirements of a Certified Person. Licensee must inform NTIS of all subsequent value-added products that are created using the Limited Access Death Master File (LADMF). To the extent possible, Licensee should include in such information products the following attribution: "Limited Access Death Master File, NTIS, U.S. Department of Commerce".

(d) Backup: Licensee may make a backup copy of the Limited Access Death Master File (LADMF) provided to it under this Agreement.

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000044

5. **Prohibited Purposes:** Except as provided in paragraph 4. above, Licensee may not:

(a) sublicense, transfer, assign, or otherwise convey any rights under this Agreement without NTIS's prior approval.

(b) make the Limited Access Death Master File (LADMF) visible, searchable, harvestable, or in any way discoverable on the World Wide Web.

(c) make duplicates, distribute, sell, commercially exploit, create derivative works from, or otherwise make available the Limited Access Death Master File (LADMF) or information contained therein, in any form or medium, to any third party.

(d) assert or authorize anyone to assert any proprietary rights to the Limited Access Death Master File (LADMF) in whole or in part or to represent the Limited Access Death Master File (LADMF) or any part of it as other than a United States Government Database;

(e) alter the specific data elements contained in Limited Access Death Master File (LADMF) or compromise its integrity, or authorize anyone else to do so, but Licensee may reformat the Limited Access Death Master File (LADMF); or

(f) make the Limited Access Death Master File (LADMF) in any form available to Licensee's employees, contractors, subcontractors, or customers who are Persons and do not meet the requirements to be a Certified Person as set forth in 15 CFR 1110.102.

6. **Security**: In order to safeguard the Limited Access Death Master File (LADMF) provided to Licensee under this Agreement, Licensee agrees that:

(a) Licensee will at all times have security provisions in place to protect the Limited Access Death Master File (LADMF) from being visible, searchable, harvestable or in any way discoverable on the World Wide Web. Licensee represents that it currently has, and will maintain for the term of this Agreement, systems, facilities, and procedures in place to safeguard all Limited Access Death Master File (LADMF), and experience in maintaining the confidentiality, security, and appropriate use of Limited Access Death Master File (LADMF), pursuant to requirements similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, agrees to satisfy the requirements of such section 6103(p)(4) as if such section applied to Licensee, and agrees to audits as set forth in this Agreement.

(b) Licensee understands that any successful attempt by any person to gain unauthorized access to or use of the Limited Access Death Master File (LADMF) from Licensee may result in immediate termination of this Agreement. In addition, any successful attempt by any person to gain unauthorized access may under appropriate circumstances result in penalties as prescribed in 15 CFR §1110.200 levied on both Licensee and the person attempting such access. Licensee will take appropriate action to ensure that all persons accessing the Limited Access Death Master File (LADMF) from Licensee are aware of their potential liability for misuse or for attempting to gain unauthorized access. Any such access or attempted access is a breach or attempted breach of security and must immediately be reported to NTIS at dmfcert@ntis.gov.

SAMPLE

AMERICAN OVERSIGHT

7. **Payment:** If Licensee does not have a current DMF subscription in place with NTIS, Licensee agrees to pay applicable fees in advance. A fee schedule is attached as Attachments A1 and A2 to this Agreement. NTIS reserves the right to change any fees set forth in Attachments A1 and A2, to establish new fees or to waive fees during the term of this Agreement by giving Licensee 90 days advance notice.

8. **Penalties:** Licensee acknowledges that failure to comply with the provisions of paragraph (3) of the Certification Form may subject the Subscriber to penalties under 15 CFR 1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

9. **Liability**: The U.S. Government/NTIS (a) makes no warranty, express or implied, with respect to information provided under this agreement, including, but not limited to, implied warranties of merchantability and fitness for any particular use; (b) assumes no liability for any direct, indirect or consequential damages flowing from any use of any part of the Limited Access Death Master File (LADMF), including infringement of third party intellectual property rights; and (c) assumes no liability for any errors or omissions in Limited Access Death Master File (LADMF). Licensee hereby waives, relinquishes and releases the U.S. Government/NTIS from any claim for damage or injury arising from its acquisition or use of the Limited Access Death Master File (LADMF) or in any products derived therefrom.

Without limiting in any way the scope and breadth of the foregoing, the parties acknowledge that the Limited Access Death Master File (LADMF) has inaccuracies and that NTIS and the Social Security Administration (SSA), which provides the LADMF to NTIS, do not guarantee the accuracy of the Limited Access Death Master File (LADMF). SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on the Limited Access Death Master File (LADMF) is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the Limited Access Death Master File (LADMF). Licensee shall include this notification in any sales or usage agreement it enters into with third-parties for the resale of the Limited Access Death Master File (LADMF) or products derived therefrom. (*See* Attachment B.)

10. **Indemnification and Hold Harmless:** To the extent not prohibited by law, Licensee shall indemnify and hold harmless the U.S. Government/NTIS from all claims, liabilities, demands, damages, expenses, and losses, whether sounding in tort, contract or otherwise, arising from or in connection with Licensee's, Licensee's employees, contractors, subcontractors, or Licensee's customers' use of the Limited Access Death Master File (LADMF). This provision shall survive termination of this Agreement and will include any and all claims or liabilities arising from intellectual property rights.

11. **Governing Law:** This Agreement will be governed by applicable Federal law.

12. **Term and Amendments:** This agreement is effective on the last date of signature by the parties below and will remain in effect for one year or, if Licensee has a current LADMF subscription in place with NTIS, the subscription expiration date, whichever is earlier. This Agreement may be renewed on an annual basis by written amendments signed by both parties for up to five years, contingent upon Licensee executing the current version of the Certification Form annually and fulfilling any and all other requirements set forth in NTIS regulations found at 15 CFR part 1110. This Agreement may be amended

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000046

at any time by a written amendment signed by both parties. Licensee must be a Certified Person throughout the term of this Agreement, and subscription will be immediately terminated if Licensee loses status as a Certified Person.

13. **Termination:** Either party may terminate the Agreement by giving the other 90 days written notice. If Licensee terminates, Licensee will not receive any refund, proration or abatement of any fees paid to NTIS. If NTIS terminates, Licensee will receive a refund for the unused portion of the Annual Fee unless Licensee is in breach of this Agreement, or has violated 15 CFR part 1110, in either case as determined by NTIS. Upon termination of this Agreement by either party, Licensee agrees to destroy all Limited Access Death Master File (LADMF) provided to Licensee by NTIS under this Agreement and will certify to NTIS in writing that is has destroyed all such Limited Access Death Master File (LADMF).

14. **Resolution of Disagreements:** Should disagreements arise on the interpretation of the provisions of this Agreement or amendments and/or revisions thereto, that cannot be resolved at the operating level, the area(s) of disagreement shall be stated in writing by each party and presented to the other party for consideration. If agreement or interpretation is not reached within 30 days, the parties shall forward the written presentation of the disagreement to respective higher officials for appropriate resolution.

Both parties agree that all claims, disputes, and/or causes of action arising under or related to this Agreement, not resolved in the dispute resolution process, shall be brought in a court/forum of competent Federal jurisdiction.

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000047

15. Contact Information:

A. Program Management:

Licensee	Primary	Alternate
Contact Name		
Organization		
Address		
Phone Number	Tel.	
Fax Number	Fax	
Email Address		
NTIS	**Primary**	**Alternate**
Contact Name	Daniel Ramsey	
Organization	National Technical Information Service (NTIS); Supervisory Program Manager, Office of Program Management, Program Control	
Address	National Technical Information Service (NTIS) 5301 Shawnee Road Alexandria, Virginia 22312	
Phone Number	703-605-6703	
Fax Number	703-605-6372	
Email Address	dramsey@ntis.gov	

SAMPLE

AMERICAN OVERSIGHT

B. Financial:

Licensee	Primary	Alternate
Contact Name		
Organization		
Address		
Phone Number		
Fax Number		
Email Address		
NTIS	**Primary**	**Alternate**
Contact Name	Office of Accounting	Office of Accounting
Organization	NTIS Accounting	NTIS Accounting
Address	5301 Shawnee Road Alexandria, VA 22312	5301 Shawnee Road Alexandria, VA 22312
Phone Number	703-605-6600	703-605-6600
Fax Number	703-605-6743	703-605-6743
Email Address	lharper@ntis.gov	cscott@ntis.gov

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000049

LICENSEE:

_____ _____
Authorized Signature Date
Name:
(License Administrator if different from above):
Corporate Name:
Address:
Phone Number:
NTIS Subscription Number:
NTIS Certification Invoice/Confirmation Number:

SAMPLE

Fax this document to:
703-605-6880
National Technical Information Service
U.S. Department of Commerce
5301 Shawnee Rd.
Alexandria, VA 22312

Attachments A1 and A2: Limited Access Death Master File Use and Resale Order Form
Attachment B: Important Information – Mandatory Requirements Death Master File

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000050

IMPORTANT INFORMATION - MANDATORY REQUIREMENTS – LIMITED ACCESS DEATH MASTER FILE

TO ALL SUBSCRIBERS PURCHASING THE SOCIAL SECURITY ADMINISTRATION'S LIMITED ACCESS DEATH MASTER FILE (LADMF):

As a result of a court case under the Freedom of Information Act, SSA is required to release its death information to the public. SSA's Limited Access Death Master File (LADMF)contains the complete and official Social Security Administration (SSA) database extract, as well as updates to the full file of persons reported to SSA as being deceased. SSA authorizes the use of this database as an identity verification tool. However, you, as a subscriber/purchaser of SSA's (LADMF) are advised at the time of initial purchase that the LADMF does have inaccuracies and SSA DOES NOT GUARANTEE THE ACCURACY OF THE LADMF FILE. SSA does not have a death record for all deceased persons. Therefore, the absence of a particular person on this file is not proof that the individual is alive. Further, in rare instances, it is possible for the records of a person who is not deceased to be included erroneously in the LADMF. If an individual seeing your copy of the LADMF has a complaint that they find erroneous data/death information on that LADMF, you should advise them to follow the procedures listed below. In fact, you should be providing the information below in your publication, if any, of the LADMF:

ERRORS - If an individual claims that SSA has incorrectly listed someone as deceased (or has incorrect dates/data on the Limited Access Death Master File (LADMF), the individual should be told to contact their local social security office (with proof) to have the error corrected. The local social security office will:

(1) make the correction to the main NUMIDENT file at SSA and give the individual a verification document of SSA's current records to use to show to any company, recipient/ purchaser of the LADMF that had the error, OR,

(2) find that SSA already has the correct information on the main NUMIDENT file and LADMF (probably corrected sometime prior), and give the individual a verification document of SSA's records to use to show to any company, subscriber/purchaser of the LADMF that had the error.

In the latter case (2 above), the LADMF subscriber (you) probably received the incorrect death data sometime prior to the correction on SSA's main records. (The only way you can now get an updated LADMF with the correction would be to again purchase the entire LADMF file and keep it current with all of the MONTHLY OR WEEKLY UPDATES - See MANDATORY REQUIREMENTS below). You should accept proof from the individual (their own records or the verification s/he received from the local social security office) and correct your copy of the LADMF. You should also notify any organizations to which you sold the LADMF that this correction needs to be made.

SAMPLE

AMERICAN OVERSIGHT

MANDATORY REQUIREMENTS:

It is mandatory that all subscribers of the LADMF intending to use its data on a continuing basis must, after receiving an updated complete LADMF FULLFILE keep that file updated by continually purchasing all MONTHLY OR WEEKLY UPDATES (NEW DEATHS/ CHANGES/DELETIONS), beginning with the same month as the Full File. If you are not meeting SSA's requirements because you are not receiving the MONTHLY OR WEEKLY UPDATES ON A CONTINUING BASIS immediately after receiving the FULL FILE, then you are NOT keeping your LADMF up-to-date with SSA's records. Thus, you are working with a LADMF with an increased number of unnecessary inaccuracies and possibly adversely affecting an increased number of individuals. NO ONE IS TO SELL THE LADMF WITHOUT REQUIRING CONTINUOUS SUBSCRIBERS TO ADHERE TO THIS MANDATORY REQUIREMENT FOR KEEPING THEIR LADMF UP-TO-DATE.

YOU, AS A LADMF SUBSCRIBER, ARE REMINDED THAT YOU SHOULD NOT TAKE ANY ADVERSE ACTION AGAINST ANY INDIVIDUAL WITHOUT FURTHER INVESTIGATION TO VERIFY THE DEATH LISTED.

If you, as a subscriber to SSA's LADMF, are making available/selling SSA's LADMF information to others, you MUST ALSO PROVIDE THEM WITH A COPY OF THIS NOTICE.

NOTE: DO NOT TELL ANYONE TO CONTACT NTIS OR SSA HEADQUARTERS FOR CORRECTIONS! CORRECTIONS MUST BE MADE AT THE LOCAL SOCIAL SECURITY OFFICE SERVICING THE INDIVIDUAL.

SAMPLE

AMERICAN OVERSIGHT

U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

Check applicable box:

☐ First time certification
☐ Renewal of certification

Limited Access Death Master File
Certification Form

1. The undersigned hereby certifies that access to the NTIS Limited Access Death Master File, (LADMF) (as defined in 15 CFR § 1110.2) is appropriate because the undersigned (a) has (i) a legitimate fraud prevention interest, or (ii) a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty, (b) has systems facilities, and procedures in place to safeguard such information, and experience in maintaining the confidentiality, security, and appropriate use of such information, pursuant to requirements reasonably similar to the requirements of section 6103(p)(4) of the Internal Revenue Code of 1986, and (c) agrees to satisfy such similar requirements.
2. In making the certification in paragraph (1) above, the undersigned states the following specific basis (must check each basis relied upon and must specify):

☐ **Fraud Prevention Interest** (explain what kind of fraud is being prevented)**:**

☐ **Business Purpose:**

☐ *Law* (cite the Law, e.g., 000 U.S.C. 0000, or applicable state or local law):

☐ *Governmental Rule* (cite the Rule):

☐ *Regulation* (cite the Regulation)*:*

☐ *Fiduciary Duty* (explain what the fiduciary duty is)*:*

3. The undersigned further certifies that with respect to LADMF of any deceased individual at any time during the three calendar year period beginning on the date of the individual's death, which is received by the undersigned, the undersigned shall not: (i) disclose any information contained on the LADMF with respect to any deceased individual to any person other than a person who meets the requirements of each of (a), (b), and (c) in paragraph (1); (ii) disclose any information contained on the LADMF with respect to any deceased individual to any person who uses the information for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation, or fiduciary duty; (iii) disclose any information contained on the LADMF with respect to any deceased individual to any person who further discloses the information to any person other than a person who meets the requirements of each of (a) and (b) in paragraph (1); or (iv) use any information contained on the LADMF with respect to any deceased individual for any purpose other than a legitimate fraud prevention interest or a legitimate business purpose pursuant to a law, governmental rule, regulation or fiduciary duty.

SAMPLE

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000058

U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

Limited Access Death Master File
Certification Form Continued

4. In making the certification in paragraph (3), the undersigned states the following (must check basis relied upon and specify in the space provided):

☐ A **The undersigned shall not disclose any information contained on the DMF with respect to any deceased individual at any time during the three-calendar-year period beginning on the date of the individual's death, which is received by the undersigned, to any other person; or**

☐ B **The undersigned will disclose information contained on the DMF with respect to an individual during the three-calendar-year period beginning on the date of the individual's death, which is received by the undersigned, to another person(s) in the following manner only (for a disclosure to another person other than a Certified Person as defined in 15 CFR § 1110.2, must also check and complete *i.* & *ii.* below)**

☐ ***i.*** **The undersigned shall ensure compliance by such other person(s) with the requirements of each of (i), (ii) and (iii) of the paragraph above as follows:**

☐ ***ii.*** **The undersigned shall ensure that such other person(s) is made aware that the penalty provisions of 15 CFR § 1110.200 apply to such person(s) as follows:**

5. The undersigned acknowledges that failure to comply with the provisions of paragraph (3) may subject the undersigned to penalties under 15 CFR §1110.200 of $1,000 for each disclosure or use, up to a maximum of $250,000 in penalties per calendar year.

6. The undersigned hereby consents to the performance by a third party auditor of periodic and unscheduled audits of the undersigned to determine the compliance by the undersigned with the certifications made herein.

7. If the undersigned makes this certification on behalf of a corporation, company, association, firm, partnership, society, joint stock company, other private organization, or state or local government department or agency, then the undersigned hereby represents and warrants that the undersigned is authorized to make this certification on behalf of, and to bind, such corporation, company, association, firm, partnership, society, joint stock company, other private organization, or state or local government department or agency.

8. The undersigned hereby declares that all certifications and statements made herein of the undersigned's own knowledge are true and that all certifications and statements made on information and belief are believed to be true; and further that these certifications and statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. §1001. The undersigned hereby acknowledges that any willful false certification or statement made herein is punishable under 18 U.S.C. §1001 by fine or imprisonment of not more than five (5) years, or both.

9. The undersigned acknowledges that, if approved, their Certification will be effective on the effective date indicated in the approval email from NTIS and will expire one year thereafter on the expiration date indicated in the same email.

SAMPLE

U.S. Department of Commerce
National Technical Information Service
Alexandria, VA 22312

Limited Access Death Master File
Certification Form Continued

Authorized Name: _____

Authorized Signature: _____

Name of corporation, company, association, firm, partnership, society, joint stock company, other private organization, or state or local government department or agency: _____

_____

Address: _____

Phone Number: _____ **Date:** _____

Death Master File Subscription: _____ **Email:** _____

NTIS Invoice/Order Confirmation Number for Processing Fee: _____

NTIS Customer Number (Customer Number assigned to you by NTIS if applicable): _____

State Incorporation/Registration Number: _____ EIN (if applicable): _____

URL (if applicable): _____

Check if applicable:

- ☐ **We are a state or local government department or agency.**
- ☐ **We are not submitting a written attestation under 15 CFR §1110.101 (b) because we are renewing our certification and;**
  - ☐ **have submitted a written attestation within three years of the date of this application.**
  - ☐ **were subject to a satisfactory audit under 15 CFR §1110.201 within three years of the date of this application.**

This collection of information contains Paperwork Reduction Act (PRA) requirements approved by the Office of Management and Budget (OMB). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the PRA unless that collection of information displays a currently valid OMB control number. Public reporting burden for this collection is estimated to be 2.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed and completing and reviewing the collection of information. Send comments regarding this burden estimate or any aspect of this collection of information, including suggestions for reducing this burden, to the National Technical Information Service, Attn: Daniel Ramsey, National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312; dramsey@ntis.gov, (703-605-6703).
OMB Control Number: 0692-0013
Expiration Date: 03/31/2023

National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312-2312

Email: DMFCERT@NTIS.GOV
Fax: 703.605.6900

SAMPLE
AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000055

From: Election Insight <newsletter@smartmatic.com>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 5/4/2023 8:57:25 AM
Subject: What does AI say about AI in elections? We asked ChatGPT.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Talking Elections with ChatGPT

We wanted to see just how much ChatGPT knows about elections – so we asked it – about everything from AI use in elections to election integrity. And if you don't know what ChatGPT is … well, you're going to want to read this to find out.

READ MORE

Fact-Checkers Are Scrambling to Fight Disinformation With AI

Bad actors use artificial intelligence to propagate falsehoods and upset elections, but the same tools can be repurposed to defend the truth.

Read more

"Artificial Intelligence and Electoral Integrity" - 19th European Conference of Electoral Management Bodies

"Artificial Intelligence and Electoral Integrity" was the topic of this year's European Conference of Electoral Management Bodies, organized by the Venice Commission.

Read more

AMERICAN OVERSIGHT

The Unglamorous Side of Election Success

Diligence to chain-of-custody, maintenance and warehousing will yield rewards when the next election rolls around.

Read more

AI Enhances Women's Participation in Electoral Processes

The High National Election Commission launched the first training in Libya for monitoring online violence against women in elections.

Read more

These are the 5 Cybersecurity Pillars to Protect an Election. Watch the video

CLICK HERE

Election Insight is powered by Smartmatic

Unsubscribe from this mailing list.

AMERICAN OVERSIGHT

From: Peters, Chrissy <chrissy.peters@sos.mo.gov>
To: Nodaway County Clerk <nodclerk@gmail.com>
Dean, Kali <Kali.Dean@sos.mo.gov>
Date: 3/13/2023 5:12:21 PM
Subject: Re: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX
Attachments: image001.jpg
image001 (1).jpg
image001 (2).jpg
Poll Book - Nov 2020 (Dobson).pdf

Hi Melinda,

You can give Kali a call and she help you with modifying voter history for past elections. You can either call the main elections line or the MCVR help desk.

You have to keep election materials for 22 months. I know the Secretary asked counties to keep the 2020 election material until we could get some clarification. There is a petition on court in Greene County and we have not received clarification at this point from that petition.

Let me know if you have any other questions. Thank you!

Chrissy Peters
Director of Elections

> On Mar 10, 2023, at 8:49 AM, Nodaway County Clerk <nodclerk@gmail.com> wrote:
>
> **CAUTION:** This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.
> Chrissy-
>
> I had Angie go pull the signature page from the November 2020 Election that Aaron Joseph Dobson would have signed. It appears WE marked the wrong person in MCVR. If you look, DeStefano, Thomas is NOT marked as voted and should have been. I would say we clicked Mr. Dobson instead. (See attached signature page.)
>
> Is this something that can be corrected? The election is closed, so I assume we cannot do it?
>
> Additionally, how long are we looking to keep the November 2020 election stuff? Am I able to get rid of unvoted ballots to free up some space?
>
> As always, thank you for your assistance in these matters.
>
> Melinda Patton
> Nodaway County Clerk
> 403 N Market
> Maryville, MO 64468
> 660-582-2251
> 660-582-5282 (fax)

AMERICAN OVERSIGHT

On Thu, Mar 9, 2023 at 8:24 AM Nodaway County Clerk <nodclerk@gmail.com> wrote:

> Thank you for the response.
>
> We have him back marked Inactive for Returned Mail in April of 2022. Should we do any kind of follow up? If he were to come in and vote in the April election, that would move him back to active. This has brought up several questions for us on our process for items like returned mail, NVRA, etc. If there is any kind of future trainings, we would be very interested.
>
> Melinda Patton
> Nodaway County Clerk
> 403 N Market
> Maryville, MO 64468
> 660-582-2251
> 660-582-5282 (fax)
>
> On Thu, Mar 9, 2023 at 8:14 AM Nodaway County <Nodaway.County@sos.mo.gov> wrote:
>
> > ---
> >
> > From: Peters, Chrissy
> > Sent: Thursday, March 9, 2023 8:14:45 AM (UTC-06:00) Central Time (US & Canada)
> > To: Nodaway County
> > Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX
> >
> > Melinda,
> >
> > Our office contacted Ian directly to discuss the complaint process with our office. He should be filing with us. We will contact you if we have any questions but we would typically work directly with the other state. Normally when we look into these situations we may need to request from you a signature from the poll book or absentee ballot envelope. We will let you know if we need to take next steps. Thank you!
> >
> > **Chrissy Peters** | **Director of Elections**
> >
> > Missouri Secretary of State Jay Ashcroft
> >
> > 600 West Main Street | Jefferson City, MO 65102
> >
> > Phone: (573) 526-3986 | 1-800-669-8683

From: Peters, Chrissy
Sent: Monday, March 6, 2023 10:01 AM
To: Nodaway County <Nodaway.County@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Thank you Melinda,

We are going to look into this. I will follow up soon.

Chrissy Peters | Director of Elections

Missouri Secretary of State Jay Ashcroft

600 West Main Street | Jefferson City, MO 65102

Phone: (573) 526-3986 | 1-800-669-8683

From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

AMERICAN OVERSIGHT

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton

Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of Texas and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON

dob: [redacted]

AMERICAN OVERSIGHT

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]

dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]

dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

AMERICAN OVERSIGHT

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted]1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.

Please confirm receipt of this email.

All The Best,

Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

AMERICAN OVERSIGHT



AMERICAN OVERSIGHT



AMERICAN OVERSIGHT



AMERICAN OVERSIGHT

County: Nodaway
Polling Places List

Printed Date : 10/29/2020
Processed Date: 10/29/2020 4:46:20 PM

VOTER'S IDENTIFICATION CERTIFICATE. Warning: It is against the law for anyone to vote, or attempt to vote, without having a lawful right to vote.

Location: CHURCH OF THE NAZARENE, LOCATION #: 17, ELECTION: NOVEMBER 2020 GENERAL ELECTION, TYPE: GENERAL, DATE: 11/3/2020

I hereby certify that I am qualified to vote at this election by signing my name and verifying my address by signing my initials next to my address.

Voter ID Status|Reason	Voter Name Residential|Mailing Address	Voter's Initials	Voter Signature	Ballot Style Precinct/Split	Judge's Initials	Seq No
45566479 Active 1368645946	**DISTEFANO,LISA GORRY** (R) 1014 GARD ST,MARYVILLE, MO 64468 (M)		[redacted]	3 POLK E (MARYVILLE)/01	BG	0853
752066017 Active ID Verification 1368645947	**DISTEFANO,THOMAS** (R) 1014 GARD ST,MARYVILLE, MO 64468 (M) TD		[redacted]	3 POLK E (MARYVILLE)/01	BG	0854
44750439 Inactive NVRA 1368645948	**DOBSON,AARON JOSEPH** (R) 1207 PARKDALE RD,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
751264412 Active 1368645949	**DOLIN,ADANNA MARISSA NICOLE** (R) 426 W LIEBER,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
751498531 Inactive NVRA 1368645950	**DONALDSON,KATHLEAN NIKIAH** (R) 2706 S MAIN ST LOT 2,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
45562123 Active 1368645951	**DORREL,JERRY DEE** (R) 1007 S DUNN,MARYVILLE, MO 64468 (M)		ABSENTEE RECEIVED	3 POLK E (MARYVILLE)/01		
45562142 Active 1368645952	**DORREL,TRUDY A** (R) 1007 S DUNN,MARYVILLE, MO 64468 (M)		ABSENTEE RECEIVED	3 POLK E (MARYVILLE)/01		
751207908 Active 1368645953	**DOUGAN,CHRISTOPHER JOE** (R) 28305 ICON RD,MARYVILLE, MO 64468 (M) CD		[redacted]	3 POLK E (MARYVILLE)/02	CB	0752

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000068

From:	Nodaway County Clerk <nodclerk@gmail.com>
To:	Peters, Chrissy <chrissy.peters@sos.mo.gov>
	Nodaway County <Nodaway.County@sos.mo.gov>
CC:	Angie Cordell <acordell@nodawaycountymo.us>
Date:	3/10/2023 8:47:40 AM
Subject:	Re: FW: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX
Attachments:	Poll Book - Nov 2020 (Dobson).pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Chrissy-

I had Angie go pull the signature page from the November 2020 Election that Aaron Joseph Dobson would have signed. It appears WE marked the wrong person in MCVR. If you look, DeStefano, Thomas is NOT marked as voted and should have been. I would say we clicked Mr. Dobson instead. (See attached signature page.)

Is this something that can be corrected? The election is closed, so I assume we cannot do it?

Additionally, how long are we looking to keep the November 2020 election stuff? Am I able to get rid of unvoted ballots to free up some space?

As always, thank you for your assistance in these matters.

Melinda Patton
Nodaway County Clerk
403 N Market
Maryville, MO 64468
660-582-2251
660-582-5282 (fax)

On Thu, Mar 9, 2023 at 8:24 AM Nodaway County Clerk <nodclerk@gmail.com> wrote:

> Thank you for the response.
>
> We have him back marked Inactive for Returned Mail in April of 2022. Should we do any kind of follow up? If he were to come in and vote in the April election, that would move him back to active. This has brought up several questions for us on our process for items like returned mail, NVRA, etc. If there is any kind of future trainings, we would be very interested.
>
> Melinda Patton
> Nodaway County Clerk
> 403 N Market
> Maryville, MO 64468
> 660-582-2251
> 660-582-5282 (fax)
>
> On Thu, Mar 9, 2023 at 8:14 AM Nodaway County <Nodaway.County@sos.mo.gov> wrote:

AMERICAN OVERSIGHT

From: Peters, Chrissy
Sent: Thursday, March 9, 2023 8:14:45 AM (UTC-06:00) Central Time (US & Canada)
To: Nodaway County
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Melinda,

Our office contacted Ian directly to discuss the complaint process with our office. He should be filing with us. We will contact you if we have any questions but we would typically work directly with the other state. Normally when we look into these situations we may need to request from you a signature from the poll book or absentee ballot envelope. We will let you know if we need to take next steps. Thank you!

Chrissy Peters | **Director of Elections**

Missouri Secretary of State Jay Ashcroft

600 West Main Street | Jefferson City, MO 65102

Phone: (573) 526-3986 | 1-800-669-8683

Missouri Secretary of State
Elections

From: Peters, Chrissy
Sent: Monday, March 6, 2023 10:01 AM
To: Nodaway County <Nodaway.County@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Thank you Melinda,

We are going to look into this. I will follow up soon.

Chrissy Peters | **Director of Elections**

Missouri Secretary of State Jay Ashcroft

600 West Main Street | Jefferson City, MO 65102

Phone: (573) 526-3986 | 1-800-669-8683

AMERICAN OVERSIGHT

Missouri Secretary of State
Elections

From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton

Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of

AMERICAN OVERSIGHT

Texas and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON

dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]

dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]

dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON

AMERICA FIRST OVERSIGHT

1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted]f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted]1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.

Please confirm receipt of this email.

AMERICAN OVERSIGHT

All The Best,

Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

County: Nodaway
Polling Places List

Printed Date : 10/29/2020
Processed Date: 10/29/2020 4:46:20 PM

VOTER'S IDENTIFICATION CERTIFICATE. Warning: It is against the law for anyone to vote, or attempt to vote, without having a lawful right to vote.

Location: CHURCH OF THE NAZARENE, LOCATION #: 17, ELECTION: NOVEMBER 2020 GENERAL ELECTION, TYPE: GENERAL, DATE: 11/3/2020

I hereby certify that I am qualified to vote at this election by signing my name and verifying my address by signing my initials next to my address.

Voter ID Status|Reason	Voter Name Residential|Mailing Address	Voter's Initials	Voter Signature	Ballot Style Precinct/Split	Judge's Initials	Seq No
45566479 Active 1368645946	**DISTEFANO,LISA GORRY** (R) 1014 GARD ST,MARYVILLE, MO 64468 (M)		[redacted]	3 POLK E (MARYVILLE)/01	BG	0853
752066017 Active ID Verification 1368645947	**DISTEFANO,THOMAS** (R) 1014 GARD ST,MARYVILLE, MO 64468 (M) TD		[redacted]	3 POLK E (MARYVILLE)/01	BG	0854
44750439 Inactive NVRA 1368645948	**DOBSON,AARON JOSEPH** (R) 1207 PARKDALE RD,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
751264412 Active 1368645949	**DOLIN,ADANNA MARISSA NICOLE** (R) 426 W LIEBER,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
751498531 Inactive NVRA 1368645950	**DONALDSON,KATHLEAN NIKIAH** (R) 2706 S MAIN ST LOT 2,MARYVILLE, MO 64468 (M)		X_____	3 POLK E (MARYVILLE)/01		
45562123 Active 1368645951	**DORREL,JERRY DEE** (R) 1007 S DUNN,MARYVILLE, MO 64468 (M)		ABSENTEE RECEIVED	3 POLK E (MARYVILLE)/01		
45562142 Active 1368645952	**DORREL,TRUDY A** (R) 1007 S DUNN,MARYVILLE, MO 64468 (M)		ABSENTEE RECEIVED	3 POLK E (MARYVILLE)/01		
751207908 Active 1368645953	**DOUGAN,CHRISTOPHER JOE** (R) 28305 ICON RD,MARYVILLE, MO 64468 (M) CD		[redacted]	3 POLK E (MARYVILLE)/02	CB	0752

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000075

From: Nodaway County Clerk <nodclerk@gmail.com>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Nodaway County <Nodaway.County@sos.mo.gov>
CC: Angie Cordell <acordell@nodawaycountymo.us>
Date: 3/9/2023 8:24:26 AM
Subject: Re: FW: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Thank you for the response.

We have him back marked Inactive for Returned Mail in April of 2022. Should we do any kind of follow up? If he were to come in and vote in the April election, that would move him back to active. This has brought up several questions for us on our process for items like returned mail, NVRA, etc. If there is any kind of future trainings, we would be very interested.

Melinda Patton
Nodaway County Clerk
403 N Market
Maryville, MO 64468
660-582-2251
660-582-5282 (fax)

On Thu, Mar 9, 2023 at 8:14 AM Nodaway County <Nodaway.County@sos.mo.gov> wrote:

> From: Peters, Chrissy
> Sent: Thursday, March 9, 2023 8:14:45 AM (UTC-06:00) Central Time (US & Canada)
> To: Nodaway County
> Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX
>
> Melinda,
>
> Our office contacted Ian directly to discuss the complaint process with our office. He should be filing with us. We will contact you if we have any questions but we would typically work directly with the other state. Normally when we look into these situations we may need to request from you a signature from the poll book or absentee ballot envelope. We will let you know if we need to take next steps. Thank you!
>
> **Chrissy Peters | Director of Elections**
>
> Missouri Secretary of State Jay Ashcroft
>
> 600 West Main Street | Jefferson City, MO 65102
>
> Phone: (573) 526-3986 | 1-800-669-8683

Missouri Secretary of State Elections

AMERICA OVERSIGHT

From: Peters, Chrissy
Sent: Monday, March 6, 2023 10:01 AM
To: Nodaway County <Nodaway.County@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Thank you Melinda,

We are going to look into this. I will follow up soon.

Chrissy Peters | Director of Elections

Missouri Secretary of State Jay Ashcroft

600 West Main Street | Jefferson City, MO 65102

Phone: (573) 526-3986 | 1-800-669-8683



From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton

AMERICAN OVERSIGHT

Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of Texas and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON

dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]

dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

AMERICAN OVERSIGHT

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
do [redacted]

dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17
(MO)

AMERICAN OVERSIGHT

[redacted]1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.

Please confirm receipt of this email.

All The Best,

Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

From: Peters, Chrissy
To: Nodaway County <Nodaway.County@sos.mo.gov>
Date: 3/9/2023 8:14:45 AM
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Melinda,
Our office contacted Ian directly to discuss the complaint process with our office. He should be filing with us. We will contact you if we have any questions but we would typically work directly with the other state. Normally when we look into these situations we may need to request from you a signature from the poll book or absentee ballot envelope. We will let you know if we need to take next steps. Thank you!

Chrissy Peters | **Director of Elections**
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683
Missouri Secretary of State
Elections

From: Peters, Chrissy
Sent: Monday, March 6, 2023 10:01 AM
To: Nodaway County <Nodaway.County@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Thank you Melinda,
We are going to look into this. I will follow up soon.

Chrissy Peters | **Director of Elections**
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683
Missouri Secretary of State
Elections

From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton

Nodaway County Clerk

AMERICAN OVERSIGHT

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of Texas and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON
dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]
dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]
dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

AMERICAN OVERSIGHT

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted] 1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.

Please confirm receipt of this email.

All The Best,
Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: Gannon, Patrick <Patrick.Gannon@ncsbe.gov>
CC: Elections-1 <Elections-1@sos.mo.gov>
SVC_SBOE.Elections <Elections.SBOE@ncsbe.gov>
Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Date: 3/6/2023 4:34:06 PM
Subject: Re: [External] One set of records involving MO and NC that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Thanks Patrick!

==========

Totes Legit Votes
A citizen election integrity analyst

On Mon, Mar 6, 2023 at 3:31 PM Gannon, Patrick <Patrick.Gannon@ncsbe.gov> wrote:

> Received and forwarded to the appropriate individuals at the State Board of Elections.
>
> Thanks,
>
> Pat

Patrick Gannon

Public Information Director

O: (919) 814-0765

M: (984) 204-0767

NORTH CAROLINA
STATE BOARD OF ELECTIONS

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Monday, March 6, 2023 2:59 PM
To: elections@sos.mo.gov; SVC_SBOE.Elections <Elections.SBOE@ncsbe.gov>
Cc: chrissy.peters@sos.mo.gov; Info@sos.mo.gov; Gannon, Patrick <Patrick.Gannon@ncsbe.gov>
Subject: [External] One set of records involving MO and NC that needs additional inspection.

CAUTION: External email. Do not click links or open attachments unless you verify. Send all suspicious email as an attachment to Report Spam.

Hello Missouri and North Carolina!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

NC CRAVEN BD142273

CHESNY, EDWARD JOESPH III
dob: [redacted]
mailaddr: 95 TIMBER CREEK DR O FALLON MO 63368
voter-history: 25 CRAVEN 000000151277 11/03/2020 11/03/2020 GENERAL ABSENTEE BY MAIL 02 HAVELOCK BD142273 25 CRAVEN 22 22
-- and --
MO ST. CHARLES 751843151
CHESNY, EDWARD JOSEPH III
[redacted]
95 TIMBER CREEK DR O FALLON MO 63368-8179 SAINT CHARLES
voter-history: 2020 General Election Voted
-- more info --
[redacted]44e97b4-26bf-4e33-add3-7b381d2b9127?obtained_at=2022-11-08

Note the JOSEPH / JOESPH misspelling in the NC voter rolls.

==========

AMERICAN OVERSIGHT

Totes Legit Votes

A citizen election integrity analyst

From: Gannon, Patrick <Patrick.Gannon@ncsbe.gov>
To: Totes Legit <toteslegitvotes@gmail.com>
Elections-1 <Elections-1@sos.mo.gov>
SVC_SBOE.Elections <Elections.SBOE@ncsbe.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Date: 3/6/2023 4:31:51 PM
Subject: RE: [External] One set of records involving MO and NC that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Received and forwarded to the appropriate individuals at the State Board of Elections.

Thanks,

Pat

Patrick Gannon
Public Information Director
O: (919) 814-0765
M: (984) 204-0767
NORTH CAROLINA
STATE BOARD OF ELECTIONS

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Monday, March 6, 2023 2:59 PM
To: elections@sos.mo.gov; SVC_SBOE.Elections <Elections.SBOE@ncsbe.gov>
Cc: chrissy.peters@sos.mo.gov; Info@sos.mo.gov; Gannon, Patrick <Patrick.Gannon@ncsbe.gov>
Subject: [External] One set of records involving MO and NC that needs additional inspection.

CAUTION: External email. Do not click links or open attachments unless you verify. Send all suspicious email as an attachment to Report Spam.

Hello Missouri and North Carolina!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the2020GE.

Please let me know you have received this email.

NC CRAVEN BD142273
CHESNY, EDWARD JOESPH III
dob: [redacted]
mailaddr: 95 TIMBER CREEK DR O FALLON MO 63368
voter-history: 25 CRAVEN 000000151277 11/03/2020 11/03/2020 GENERAL ABSENTEE BY MAIL 02 HAVELOCK BD142273 25 CRAVEN 22 22
-- and --
MO ST. CHARLES 751843151
CHESNY, EDWARD JOSEPH III
[redacted]

AMERICAN OVERSIGHT

95 TIMBER CREEK DR O FALLON MO 63368-8179 SAINT CHARLES
voter-history: 2020 General Election Voted
-- more info --
[redacted]44e97b4-26bf-4e33-add3-7b381d2b9127?obtained_at=2022-11-08

Note the JOSEPH / JOESPH misspelling in the NC voter rolls.

==========

Totes Legit Votes
A citizen election integrity analyst

From: Peters, Chrissy
To: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Winn, Jody <Jody.Winn@sos.mo.gov>
Date: 3/6/2023 3:33:11 PM
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Thank you for the information Rachel.

Chrissy Peters | **Director of Elections**
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683

Missouri Secretary of State
Elections

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Monday, March 6, 2023 2:59 PM
To: Winn, Jody <Jody.Winn@sos.mo.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello again, Please ignore this last request, I have now learned from Wagoner County Election Board here in Oklahoma that this was additional case of another voter signing the wrong line on the precinct registry and applying voter history credit to the wrong individual. Therefore, I don't think it is necessary to obtain your records any longer. I appreciate your willingness to get us the records.
Sincerely,
Rachel

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

Learn more about the security and integrity of Oklahoma's elections:
https://oklahoma.gov/elections/security-integrity.html

From: Rachel Rogers
Sent: Monday, March 6, 2023 12:29 PM
To: Winn, Jody <Jody.Winn@sos.mo.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Good Morning Jody,
Thanks for getting back to me!

I will let you know that I have since heard back from the Tulsa County Election Board regarding WELLBORN, MATTHEW THOMAS and KENSEY M JOHNSON – and neither of those individuals appeared to have voted in Oklahoma in the 2020

AMERICAN OVERSIGHT

General Election. That only leaves the other voter below in which I may need records for. I don't have a GoTo meetings application here in Oklahoma. Would it be possible to email whatever screenshots or information you have regarding BROWN, CARSON PENN and their voting records? Thanks so much!

Rachel

From: Winn, Jody <Jody.Winn@sos.mo.gov>
Sent: Monday, March 6, 2023 10:09 AM
To: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Rachel,

Good morning, I am working on getting the information for you. As soon as I get everything together I will contact you to set up a GoTo meeting so that we can share screens and print off the information needed.

Thank you,

Jody Winn
Elections Specialist
Missouri Secretary of State Jay Ashcroft
600 W. Main St.|Jefferson City, MO 65102
Phone: 573-522-0306 | 800-669-8683
Fax# 573-526-3242
jody.winn@sos.mo.gov

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Thursday, March 2, 2023 3:34 PM
To: Elections-1 <Elections-1@sos.mo.gov>
Cc: SOSMain <sosmain@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning,

I am from the Oklahoma State Election Board and I am gathering up information related to this complaint to give to our state and local law enforcement partners. Could someone from your office please provide copies of any pertinent voter registration and voter records related to these matters? I would be glad to share any of our records you may wish to review as well. Attached are our voter history credit reports from our election system indicating all three did vote in person here in Oklahoma.

Thank you!

Sincerely,

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28

AMERICAN OVERSIGHT

State Capitol Building
rrogers@elections.ok.gov
405.521.6962

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Thursday, March 2, 2023 2:36 PM
To: elections@sos.mo.gov; Elections Info <Info@elections.ok.gov>
Cc: Info@sos.mo.gov; Paul Ziriax <Paul.Ziriax@elections.ok.gov>
Subject: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Hello Oklahoma and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the2020GE.

Please let me know you have received this email.

OK 720755882
WELLBORN, MATTHEW THOMAS
dob: 0[redacted]
resaddr: 10507 N 90 E AVE OWASSO 74055
voter-history: 11/03/2020 IP
-- and --
MO CHRISTIAN 752064540
MATTHEW THOMAS WELLBORN
dob: [redacted]
resaddr: 1955 W MACKENZIE'S WAY NIXA MO 65714-7033 CHRISTIAN
voter-history: 2020 General Election Voted
-- detected by NCOA --
MATTHEW THOMAS WELLBORN
ncoa-from: 10507 N 90 E AVE, OWASSO, OK
ncoa-to: 1955 W MACKENZIES WAY NIXA MO 65714
ncoa-date: 2018-06-01
-- other info --
[redacted]d16e6c1-4e3b-4da7-bf47-f55aac52f2e0?obtained_at=2021-11-17
[redacted] af14aa6-9a17-4033-8188-393625d6b268?obtained_at=2021-10-20

OK 801335502
BROWN, CARSON PENN
dob: [redacted]
resaddr: 15361 S 369 E AVE COWETA 74429
voter-history: 11/03/2020 IP
-- and --
MO BOONE 752001494
CARSON P BROWN
dob: [redacted]
resaddr: 3750 E MCGEE RD COLUMBIA MO 65202-8361 BOONE
voter-history: 2020 General Election Voted
-- detected by NCOA --
CARSON PENN BROWN
ncoa-from: 15361 S 369 E AVE, COWETA, OK
ncoa-to: 3750 E MCGEE RD COLUMBIA MO 65202
ncoa-date: 2018-07-01
-- other info --
[redacted]5323202-c338-45a4-967f-38863fd98087?obtained_at=2021-10-20
[redacted]ab4a3c7a-7f77-49d8-b216-1a8c7cf47c2a?obtained_at=2021-11-17

AMERICAN OVERSIGHT

MO 35322116
KENSEY M JOHNSON
dob: [redacted]
resaddr: 5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
voter-history: 2020 General Election Voted
-- and --
OK 802769193
JOHNSON KENSEY MICHELLE
dob: [redacted]
resaddr: 18522 E 43 ST TULSA 74134
voter-history: 11/03/2020 IP
-- detected by NCOA --
KENSEY M JOHNSON
5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
18522 E 43RD ST TULSA OK 74134-5935 TULSA
10/01/2020
-- other info --
[redacted]f708fa59-d296-4e4c-9c5f-65c3b39378ad?obtained_at=2021-11-17
[redacted]bf887ab8-6180-4278-a579-89b227677465?obtained_at=2021-10-20

==========

Totes Legit Votes
A citizen election integrity analyst

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
To: Winn, Jody <Jody.Winn@sos.mo.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 3/6/2023 2:58:36 PM
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello again, Please ignore this last request, I have now learned from Wagoner County Election Board here in Oklahoma that this was additional case of another voter signing the wrong line on the precinct registry and applying voter history credit to the wrong individual. Therefore, I don't think it is necessary to obtain your records any longer. I appreciate your willingness to get us the records.
Sincerely,
Rachel

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

Learn more about the security and integrity of Oklahoma's elections:
https://oklahoma.gov/elections/security-integrity.html

From: Rachel Rogers
Sent: Monday, March 6, 2023 12:29 PM
To: Winn, Jody <Jody.Winn@sos.mo.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Good Morning Jody,
Thanks for getting back to me!

I will let you know that I have since heard back from the Tulsa County Election Board regarding WELLBORN, MATTHEW THOMAS and KENSEY M JOHNSON – and neither of those individuals appeared to have voted in Oklahoma in the 2020 General Election. That only leaves the other voter below in which I may need records for. I don't have a GoTo meetings application here in Oklahoma. Would it be possible to email whatever screenshots or information you have regarding BROWN, CARSON PENN and their voting records? Thanks so much!

Rachel

From: Winn, Jody <Jody.Winn@sos.mo.gov>
Sent: Monday, March 6, 2023 10:09 AM
To: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Rachel,

Good morning, I am working on getting the information for you. As soon as I get everything together I will contact you

AMERICAN OVERSIGHT

to set up a GoTo meeting so that we can share screens and print off the information needed.

Thank you,

Jody Winn
Elections Specialist
Missouri Secretary of State Jay Ashcroft
600 W. Main St.|Jefferson City, MO 65102
Phone: 573-522-0306 | 800-669-8683
Fax# 573-526-3242
jody.winn@sos.mo.gov

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Thursday, March 2, 2023 3:34 PM
To: Elections-1 <Elections-1@sos.mo.gov>
Cc: SOSMain <sosmain@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning,

I am from the Oklahoma State Election Board and I am gathering up information related to this complaint to give to our state and local law enforcement partners. Could someone from your office please provide copies of any pertinent voter registration and voter records related to these matters? I would be glad to share any of our records you may wish to review as well. Attached are our voter history credit reports from our election system indicating all three did vote in person here in Oklahoma.

Thank you!

Sincerely,

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Thursday, March 2, 2023 2:36 PM
To: elections@sos.mo.gov; Elections Info <Info@elections.ok.gov>
Cc: Info@sos.mo.gov; Paul Ziriax <Paul.Ziriax@elections.ok.gov>
Subject: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Hello Oklahoma and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the2020GE.

AMERICAN OVERSIGHT

Please let me know you have received this email.

OK 720755882
WELLBORN, MATTHEW THOMAS
dob: [redacted]
resaddr: 10507 N 90 E AVE OWASSO 74055
voter-history: 11/03/2020 IP
-- and --
MO CHRISTIAN 752064540
MATTHEW THOMAS WELLBORN
do [redacted]
resaddr: 1955 W MACKENZIE'S WAY NIXA MO 65714-7033 CHRISTIAN
voter-history: 2020 General Election Voted
-- detected by NCOA --
MATTHEW THOMAS WELLBORN
ncoa-from: 10507 N 90 E AVE, OWASSO, OK
ncoa-to: 1955 W MACKENZIES WAY NIXA MO 65714
ncoa-date: 2018-06-01
-- other info --
[redacted]d16e6c1-4e3b-4da7-bf47-f55aac52f2e0?obtained_at=2021-11-17
[redacted]_af14aa6-9a17-4033-8188-393625d6b268?obtained_at=2021-10-20

OK 801335502
BROWN, CARSON PENN
dob: [redacted]
resaddr: 15361 S 369 E AVE COWETA 74429
voter-history: 11/03/2020 IP
-- and --
MO BOONE 752001494
CARSON P BROWN
dob: [redacted]
resaddr: 3750 E MCGEE RD COLUMBIA MO 65202-8361 BOONE
voter-history: 2020 General Election Voted
-- detected by NCOA --
CARSON PENN BROWN
ncoa-from: 15361 S 369 E AVE, COWETA, OK
ncoa-to: 3750 E MCGEE RD COLUMBIA MO 65202
ncoa-date: 2018-07-01
-- other info --
[redacted]5323202-c338-45a4-967f-38863fd98087?obtained_at=2021-10-20
[redacted]ab4a3c7a-7f77-49d8-b216-1a8c7cf47c2a?obtained_at=2021-11-17

MO 35322116
KENSEY M JOHNSON
dob: 1[redacted]
resaddr: 5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
voter-history: 2020 General Election Voted
-- and --
OK 802769193
JOHNSON KENSEY MICHELLE
dob: [redacted]
resaddr: 18522 E 43 ST TULSA 74134
voter-history: 11/03/2020 IP
-- detected by NCOA --
KENSEY M JOHNSON

AMERICAN OVERSIGHT

5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
18522 E 43RD ST TULSA OK 74134-5935 TULSA
10/01/2020
-- other info --
[redacted]f708fa59-d296-4e4c-9c5f-65c3b39378ad?obtained_at=2021-11-17
[redacted]bf887ab8-6180-4278-a579-89b227677465?obtained_at=2021-10-20

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: Elections-1 <Elections-1@sos.mo.gov>
SVC_SBOE.Elections <elections.sboe@ncsbe.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Gannon, Patrick <Patrick.Gannon@ncsbe.gov>
Date: 3/6/2023 1:59:24 PM
Subject: One set of records involving MO and NC that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Missouri and North Carolina!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

NC CRAVEN BD142273
CHESNY, EDWARD JOESPH III
dob: [redacted]
mailaddr: 95 TIMBER CREEK DR O FALLON MO 63368
voter-history: 25 CRAVEN 000000151277 11/03/2020 11/03/2020 GENERAL ABSENTEE BY MAIL 02 HAVELOCK BD142273 25 CRAVEN 22 22
-- and --
MO ST. CHARLES 751843151
CHESNY, EDWARD JOSEPH III
[redacted]
95 TIMBER CREEK DR O FALLON MO 63368-8179 SAINT CHARLES
voter-history: 2020 General Election Voted
-- more info --
[redacted]44e97b4-26bf-4e33-add3-7b381d2b9127?obtained_at=2022-11-08

Note the JOSEPH / JOESPH misspelling in the NC voter rolls.

==========

Totes Legit Votes
A citizen election integrity analyst

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
To: Winn, Jody <Jody.Winn@sos.mo.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 3/6/2023 12:28:36 PM
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning Jody,
Thanks for getting back to me!

I will let you know that I have since heard back from the Tulsa County Election Board regarding WELLBORN, MATTHEW THOMAS and KENSEY M JOHNSON – and neither of those individuals appeared to have voted in Oklahoma in the 2020 General Election. That only leaves the other voter below in which I may need records for. I don't have a GoTo meetings application here in Oklahoma. Would it be possible to email whatever screenshots or information you have regarding BROWN, CARSON PENN and their voting records? Thanks so much!

Rachel

From: Winn, Jody <Jody.Winn@sos.mo.gov>
Sent: Monday, March 6, 2023 10:09 AM
To: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Cc: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Rachel,

Good morning, I am working on getting the information for you. As soon as I get everything together I will contact you to set up a GoTo meeting so that we can share screens and print off the information needed.

Thank you,

Jody Winn
Elections Specialist
Missouri Secretary of State Jay Ashcroft
600 W. Main St.|Jefferson City, MO 65102
Phone: 573-522-0306 | 800-669-8683
Fax# 573-526-3242
jody.winn@sos.mo.gov

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Thursday, March 2, 2023 3:34 PM
To: Elections-1 <Elections-1@sos.mo.gov>
Cc: SOSMain <sosmain@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning,

AMERICAN OVERSIGHT

I am from the Oklahoma State Election Board and I am gathering up information related to this complaint to give to our state and local law enforcement partners. Could someone from your office please provide copies of any pertinent voter registration and voter records related to these matters? I would be glad to share any of our records you may wish to review as well. Attached are our voter history credit reports from our election system indicating all three did vote in person here in Oklahoma.

Thank you!

Sincerely,

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Thursday, March 2, 2023 2:36 PM
To: elections@sos.mo.gov; Elections Info <Info@elections.ok.gov>
Cc: Info@sos.mo.gov; Paul Ziriax <Paul.Ziriax@elections.ok.gov>
Subject: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Hello Oklahoma and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

OK 720755882
WELLBORN, MATTHEW THOMAS
dob: [redacted]
resaddr: 10507 N 90 E AVE OWASSO 74055
voter-history: 11/03/2020 IP
-- and --
MO CHRISTIAN 752064540
MATTHEW THOMAS WELLBORN
dob: [redacted]
resaddr: 1955 W MACKENZIE'S WAY NIXA MO 65714-7033 CHRISTIAN
voter-history: 2020 General Election Voted
-- detected by NCOA --
MATTHEW THOMAS WELLBORN
ncoa-from: 10507 N 90 E AVE, OWASSO, OK
ncoa-to: 1955 W MACKENZIES WAY NIXA MO 65714
ncoa-date: 2018-06-01
-- other info --
[redacted]d16e6c1-4e3b-4da7-bf47-f55aac52f2e0?obtained_at=2021-11-17
[redacted] af14aa6-9a17-4033-8188-393625d6b268?obtained_at=2021-10-20

OK 801335502
BROWN, CARSON PENN
dob: [redacted]

AMERICAN OVERSIGHT

resaddr: 15361 S 369 E AVE COWETA 74429
voter-history: 11/03/2020 IP
-- and --
MO BOONE 752001494
CARSON P BROWN
dob: [redacted]
resaddr: 3750 E MCGEE RD COLUMBIA MO 65202-8361 BOONE
voter-history: 2020 General Election Voted
-- detected by NCOA --
CARSON PENN BROWN
ncoa-from: 15361 S 369 E AVE, COWETA, OK
ncoa-to: 3750 E MCGEE RD COLUMBIA MO 65202
ncoa-date: 2018-07-01
-- other info --
[redacted]5323202-c338-45a4-967f-38863fd98087?obtained_at=2021-10-20
[redacted]ab4a3c7a-7f77-49d8-b216-1a8c7cf47c2a?obtained_at=2021-11-17

MO 35322116
KENSEY M JOHNSON
dob: [redacted]
resaddr: 5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
voter-history: 2020 General Election Voted
-- and --
OK 802769193
JOHNSON KENSEY MICHELLE
dob: [redacted]
resaddr: 18522 E 43 ST TULSA 74134
voter-history: 11/03/2020 IP
-- detected by NCOA --
KENSEY M JOHNSON
5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
18522 E 43RD ST TULSA OK 74134-5935 TULSA
10/01/2020
-- other info --
[redacted]f708fa59-d296-4e4c-9c5f-65c3b39378ad?obtained_at=2021-11-17
[redacted]bf887ab8-6180-4278-a579-89b227677465?obtained_at=2021-10-20

==========

Totes Legit Votes
A citizen election integrity analyst

From: Totes Legit <toteslegitvotes@gmail.com>
To: Elections-1 <Elections-1@sos.mo.gov>
elections@sos.wa.gov
CC: Elections - VRSupport <VRSupport@sos.wa.gov>
bryn.kildow@sos.wa.gov
Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
elections@co.thurston.wa.us
Date: 3/6/2023 11:27:13 AM
Subject: One set of records involving MO and WA that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Missouri and Washington!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

WA TH 776982
ALLISON MORGAN GRAY
dob: [redacted]
mailaddr: 102 S MISSOURI ST GREEN RIDGE 65332 MO
voter-history: vote-date 2020-11-03 31|776982|2020-11-03|145834684
-- and --
MO PETTIS 752132670
ALLISON GRAY
dob: [redacted]
resaddr: 102 S MISSOURI ST GREEN RIDGE MO 65332-1131 PETTIS
voter-history: 2020 General Election Voted
-- more info --
[redacted]1e9a66fd-6429-4926-8928-566e0b9655a8?obtained_at=2021-08-18
[redacted]8a1a382-d25a-4491-b1e1-f70673e43f51?obtained_at=2021-11-17

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: OECS@dos.myflorida.com
Elections-1 <Elections-1@sos.mo.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Mercer, Kalen L. <Kalen.Mercer@dos.myflorida.com>
DivElections <DivElections@dos.myflorida.com>
SOSMain <sosmain@sos.mo.gov>
Date: 3/6/2023 10:13:53 AM
Subject: Two sets of records involving FL and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Florida and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

FL MRN 128463308
LINDSEY, MATTHEW RICHARD
dob: [redacted]
mailaddr: 1622 KNIGHTWOOD LN O'FALLON MO 63366
voter-history: MRN 128463308 11/03/2020 GEN A
-- and --
MO ST. CHARLES 46569173
LINDSEY, MATTHEW RICHARD
dob: [redacted]
resaddr: 1622 KNIGHTWOOD LN O FALLON MO 63366-1027 SAINT CHARLES
voter-history: 2020 General Election Voted
-- more info --
[redacted]c6251103-c12f-4d8e-888f-e05c1d529638?obtained_at=2022-11-01
[redacted]64e30857-adab-4bd4-bea1-e31f39344de6?obtained_at=2021-11-17

FL PAL 112639082
SANDERS, VALERIE JEAN
dob: [redacted]
mailaddr: 1251 W 62 ST KANSAS CITY MO 64113
voter-history: PAL 112639082 11/03/2020 GEN A
-- and --
MO JACKSON 25646074
SANDERS, VALERIE JEAN
dob: [redacted]
resaddr: 1251 W 62ND ST KANSAS CITY MO 64113-1510 JACKSON
voter-history: 2020 General Election Voted
-- more info --
[redacted]43377f6a-1bcf-4426-9f13-dd1c2c8a7950?obtained_at=2022-11-01
[redacted]31778606-028b-446c-a400-8217e8c0f62d?obtained_at=2021-11-17

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Winn, Jody <Jody.Winn@sos.mo.gov>
To: Rachel.Rogers@elections.ok.gov
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 3/6/2023 10:08:33 AM
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Rachel,

Good morning, I am working on getting the information for you. As soon as I get everything together I will contact you to set up a GoTo meeting so that we can share screens and print off the information needed.

Thank you,

Jody Winn
Elections Specialist
Missouri Secretary of State Jay Ashcroft
600 W. Main St.|Jefferson City, MO 65102
Phone: 573-522-0306 | 800-669-8683
Fax# 573-526-3242
jody.winn@sos.mo.gov

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Thursday, March 2, 2023 3:34 PM
To: Elections-1 <Elections-1@sos.mo.gov>
Cc: SOSMain <sosmain@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning,

I am from the Oklahoma State Election Board and I am gathering up information related to this complaint to give to our state and local law enforcement partners. Could someone from your office please provide copies of any pertinent voter registration and voter records related to these matters? I would be glad to share any of our records you may wish to review as well. Attached are our voter history credit reports from our election system indicating all three did vote in person here in Oklahoma.

Thank you!

Sincerely,

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Thursday, March 2, 2023 2:36 PM
To: elections@sos.mo.gov; Elections Info <Info@elections.ok.gov>
Cc: Info@sos.mo.gov; Paul Ziriax <Paul.Ziriax@elections.ok.gov>
Subject: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Hello Oklahoma and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

OK 720755882
WELLBORN, MATTHEW THOMAS
dob: [redacted]
resaddr: 10507 N 90 E AVE OWASSO 74055
voter-history: 11/03/2020 IP
-- and --
MO CHRISTIAN 752064540
MATTHEW THOMAS WELLBORN
dob: [redacted]
resaddr: 1955 W MACKENZIE'S WAY NIXA MO 65714-7033 CHRISTIAN
voter-history: 2020 General Election Voted
-- detected by NCOA --
MATTHEW THOMAS WELLBORN
ncoa-from: 10507 N 90 E AVE, OWASSO, OK
ncoa-to: 1955 W MACKENZIES WAY NIXA MO 65714
ncoa-date: 2018-06-01
-- other info --
[redacted]d16e6c1-4e3b-4da7-bf47-f55aac52f2e0?obtained_at=2021-11-17
[redacted] af14aa6-9a17-4033-8188-393625d6b268?obtained_at=2021-10-20

OK 801335502
BROWN, CARSON PENN
dob: [redacted]
resaddr: 15361 S 369 E AVE COWETA 74429
voter-history: 11/03/2020 IP
-- and --
MO BOONE 752001494
CARSON P BROWN
dob: [redacted]
resaddr: 3750 E MCGEE RD COLUMBIA MO 65202-8361 BOONE
voter-history: 2020 General Election Voted
-- detected by NCOA --
CARSON PENN BROWN
ncoa-from: 15361 S 369 E AVE, COWETA, OK
ncoa-to: 3750 E MCGEE RD COLUMBIA MO 65202
ncoa-date: 2018-07-01
-- other info --
[redacted]5323202-c338-45a4-967f-38863fd98087?obtained_at=2021-10-20
[redacted]ab4a3c7a-7f77-49d8-b216-1a8c7cf47c2a?obtained_at=2021-11-17

MO 35322116
KENSEY M JOHNSON

AMERICAN OVERSIGHT

dob: [redacted]
resaddr: 5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
voter-history: 2020 General Election Voted
-- and --
OK 802769193
JOHNSON KENSEY MICHELLE
dob: [redacted]
resaddr: 18522 E 43 ST TULSA 74134
voter-history: 11/03/2020 IP
-- detected by NCOA --
KENSEY M JOHNSON
5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
18522 E 43RD ST TULSA OK 74134-5935 TULSA
10/01/2020
-- other info --
[redacted]f708fa59-d296-4e4c-9c5f-65c3b39378ad?obtained_at=2021-11-17
[redacted]bf887ab8-6180-4278-a579-89b227677465?obtained_at=2021-10-20

==========

Totes Legit Votes
A citizen election integrity analyst

From: Peters, Chrissy
To: Winn, Jody <Jody.Winn@sos.mo.gov>
Date: 3/6/2023 10:02:52 AM
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Jody,
Can you please reach out to Rachel Rogers and set up a go to meeting with her…review these voters together and see what we can work on here. Thank you!

Chrissy Peters | **Director of Elections**
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683

Missouri Secretary of State
Elections

From: Elections-1 <Elections-1@sos.mo.gov>
Sent: Thursday, March 2, 2023 3:38 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Winn, Jody <Jody.Winn@sos.mo.gov>
Subject: FW: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

From: Rachel Rogers <Rachel.Rogers@elections.ok.gov>
Sent: Thursday, March 2, 2023 3:34 PM
To: Elections-1 <Elections-1@sos.mo.gov>
Cc: SOSMain <sosmain@sos.mo.gov>
Subject: RE: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good Morning,

I am from the Oklahoma State Election Board and I am gathering up information related to this complaint to give to our state and local law enforcement partners. Could someone from your office please provide copies of any pertinent voter registration and voter records related to these matters? I would be glad to share any of our records you may wish to review as well. Attached are our voter history credit reports from our election system indicating all three did vote in person here in Oklahoma.

Thank you!

Sincerely,

Rachel A. Rogers
Director of Policy and Legal Affairs
In-House Counsel
Oklahoma State Election Board
2300 Lincoln Blvd, Room G28
State Capitol Building
rrogers@elections.ok.gov
405.521.6962

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Thursday, March 2, 2023 2:36 PM
To: elections@sos.mo.gov; Elections Info <Info@elections.ok.gov>
Cc: Info@sos.mo.gov; Paul Ziriax <Paul.Ziriax@elections.ok.gov>
Subject: [EXTERNAL] Three sets of records involving OK and MO that need additional inspection.

Hello Oklahoma and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

OK 720755882
WELLBORN, MATTHEW THOMAS
dob: [redacted]
resaddr: 10507 N 90 E AVE OWASSO 74055
voter-history: 11/03/2020 IP
-- and --
MO CHRISTIAN 752064540
MATTHEW THOMAS WELLBORN
do [redacted]
resaddr: 1955 W MACKENZIE'S WAY NIXA MO 65714-7033 CHRISTIAN
voter-history: 2020 General Election Voted
-- detected by NCOA --
MATTHEW THOMAS WELLBORN
ncoa-from: 10507 N 90 E AVE, OWASSO, OK
ncoa-to: 1955 W MACKENZIES WAY NIXA MO 65714
ncoa-date: 2018-06-01
-- other info --
[redacted]d16e6c1-4e3b-4da7-bf47-f55aac52f2e0?obtained_at=2021-11-17
[redacted] af14aa6-9a17-4033-8188-393625d6b268?obtained_at=2021-10-20

OK 801335502
BROWN, CARSON PENN
dob: [redacted]
resaddr: 15361 S 369 E AVE COWETA 74429
voter-history: 11/03/2020 IP
-- and --
MO BOONE 752001494
CARSON P BROWN
dob: [redacted]
resaddr: 3750 E MCGEE RD COLUMBIA MO 65202-8361 BOONE
voter-history: 2020 General Election Voted
-- detected by NCOA --
CARSON PENN BROWN
ncoa-from: 15361 S 369 E AVE, COWETA, OK
ncoa-to: 3750 E MCGEE RD COLUMBIA MO 65202
ncoa-date: 2018-07-01
-- other info --
[redacted]5323202-c338-45a4-967f-38863fd98087?obtained_at=2021-10-20
[redacted]ab4a3c7a-7f77-49d8-b216-1a8c7cf47c2a?obtained_at=2021-11-17

MO 35322116
KENSEY M JOHNSON
dob: [redacted]

AMERICAN OVERSIGHT

resaddr: 5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
voter-history: 2020 General Election Voted
-- and --
OK 802769193
JOHNSON KENSEY MICHELLE
dob: [redacted]
resaddr: 18522 E 43 ST TULSA 74134
voter-history: 11/03/2020 IP
-- detected by NCOA --
KENSEY M JOHNSON
5370 GIBSON RD ODESSA MO 64076 LAFAYETTE
18522 E 43RD ST TULSA OK 74134-5935 TULSA
10/01/2020
-- other info --
[redacted]f708fa59-d296-4e4c-9c5f-65c3b39378ad?obtained_at=2021-11-17
[redacted]bf887ab8-6180-4278-a579-89b227677465?obtained_at=2021-10-20

==========

Totes Legit Votes
A citizen election integrity analyst

From: Peters, Chrissy
To: Nodaway County <Nodaway.County@sos.mo.gov>
Pauley, Scott <Scott.Pauley@sos.mo.gov>
Straub, Dee Dee <deedee.straub@sos.mo.gov>
Elections-1 <Elections-1@sos.mo.gov>
Date: 3/6/2023 10:00:43 AM
Subject: RE: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

Thank you Melinda,
We are going to look into this. I will follow up soon.

Chrissy Peters | Director of Elections
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683
Missouri Secretary of State
Elections

From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton

Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of Texas

AMERICAN OVERSIGHT

and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON
dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]
dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]
dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted] 1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.

AMERICAN OVERSIGHT

Please confirm receipt of this email.

All The Best,
Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: Elections-1 <Elections-1@sos.mo.gov>
Elections AZSOS <elections@azsos.gov>
voterinfo@risc.maricopa.gov
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Janine Petty - RISCX <jpetty@risc.maricopa.gov>
Date: 3/3/2023 3:04:30 PM
Subject: One set of records involving AZ and MO that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Missouri and Arizona!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

AZ MARICOPA 5036818
RICHARD LEE TREASTER
dob: [redacted]
mailaddr: PO BOX 6599 GLENDALE AZ 85312 GLENDALE AZ 85312
voter-history: GE2020 R RETURNED Early Ballot and it counted
-- and --
MO ST. FRANCOIS 751512981
RICHARD LEE TREASTER
dob: [redacted]
resaddr: 3651 CAUSEY RD FARMINGTON MO 63640
voter-history: 2020 General Election Voted
-- detected by NCOA --
RICHARD LEE TREASTER
ncoa-from: 3651 CAUSEY RD FARMINGTON MO 63640 ST. FRANCOIS
ncoa-to: PO BOX 6599 GLENDALE AZ 85312-6599 MARICOPA
ncoa-date: 10/01/2019
-- other info --
[redacted]71eac720-d9bb-4a05-bdb3-3df11fc6e74a?obtained_at=2021-11-17

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: elinfo@clarkcountynv.gov
SOS Elections Division <nvelect@sos.nv.gov>
Elections-1 <Elections-1@sos.mo.gov>
CC: Dan Kulin <DKulin@clarkcountynv.gov>
Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Date: 3/3/2023 12:35:35 PM
Subject: One set of records involving NV and MO that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Nevada and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

These matches were detected by citizen group Missouri Canvassers. I concur with the sensibility of the matches and I am relaying their report to you.

Please let me know you have received this email.

MO JACKSON 751835008
KAYLEY MICHELLE ENGLUND
dob: [redacted]
resaddr: 2109 SW CEDAR HILL LN LEES SUMMIT MO 64081
voter-history: 2020 General Election Voted
-- and --
NV CLARK 6117333 2752908 IA81541
KAYLEY MICHELLE ENGLUND
dob: [redacted]
resaddr: 2246 CALTANA CT HENDERSON NV 89052
voter-history: 11/03/2020, 20G E
-- detected by NCOA --
KAYLEY MICHELLE ENGLUND
ncoa-from: 2109 SW CEDAR HILL LN LEES SUMMIT MO 64081
ncoa-to: 2246 CALTANA CT HENDERSON NV 89052-2710 CLARK
ncoa-date: 08/01/2020
-- other info --
[redacted]c76a59f3-71ab-495b-be47-90ba9b9ca2bb?obtained_at=2022-10-28

==========

Totes Legit Votes
A citizen election integrity analyst

From: Totes Legit <toteslegitvotes@gmail.com>
To: soscontact@sos.ga.gov
Elections-1 <Elections-1@sos.mo.gov>
CC: Koth, Sara <skoth@sos.ga.gov>
Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Date: 3/2/2023 5:56:29 PM
Subject: One set of records involving GA and MO that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Georgia and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

These matches were detected by citizen group Missouri Canvassers. I concur with the sensibility of the matches and I am relaying their report to you.

Please let me know you have received this email.

MO GREENE 751535807
MIKAELA RACHELLE NEILL
dob: [redacted]
resaddr: 9595 E STATE HIGHWAY AD ROGERSVILLE MO65742
voter-history: 2020 General Election Voted
-- and --
GA 110 08644671
NEILL MIKAELA RACHELLE
dob: [redacted]
resaddr: 243 SWEETGUM TRCE DALLAS 30132
voter-history: 110 08644671 20201103 003 NNN
-- detected by NCOA --
MIKAELA RACHELLE NEILL
ncoa-from: 9595 E STATE HIGHWAY AD ROGERSVILLE MO65742 GREENE
ncoa-to: 1406 CHASEWIND CT POWDER SPRINGS GA 30127-1082 COBB
ncoa-date: 06/01/2018
-- other info --
[redacted]cc4a9718-2cd5-4ba1-a263-25fb1bf54dc2?obtained_at=2021-11-17
[redacted]705a301e-c485-4045-b1d8-8a8e3bdb0698?obtained_at=2022-11-17

==========

Totes Legit Votes
A citizen election integrity analyst

From: Totes Legit <toteslegitvotes@gmail.com>
To: Elections-1 <Elections-1@sos.mo.gov>
Public.Elections@sos.state.co.us
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
SOSMain <sosmain@sos.mo.gov>
Judd Choate <judd.choate@sos.state.co.us>
Vicky Stecklein <Vicky.Stecklein@coloradosos.gov>
Date: 3/2/2023 4:42:52 PM
Subject: One set of records involving CO and MO that needs additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Missouri and Colorado!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

MO ST. LOUIS 73063377
ANN E GRAFFY
dob: [redacted] (full DOB sanitized for CO email)
resaddr: 1553 CROSSETT DR ST LOUIS MO 63138
voter-history: 2020 General Election Voted
-- and --
CO 602326910 JEFFERSON
ANN ELIZABETH GRAFFY
resaddr: 7772 SURREY DR MORRISON CO 80465
dob: [redacted]
voter-history: 602326910 GENERAL 11/03/2020 2020 JEFFERSON COUNTY GENERAL ELECTION MAIL BALLOT JEFFERSON
-- detected by NCOA --
ANN E GRAFFY
ncoa-from: 1553 CROSSETT DR ST LOUIS MO 63138 ST. LOUIS
ncoa-to: 7772 SURREY DR MORRISON CO 80465-2403 JEFFERSON
ncoa-date: 05/01/2020
-- other info --
[redacted]90eced3-55da-47a9-b926-9bddf9307824?obtained_at=2021-11-17
[redacted]aa18a014-dc0a-4e57-9a1a-86a0923d766d?obtained_at=2022-04-21

These registrations were also detected independently by citizen group Missouri Canvassers.

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Totes Legit <toteslegitvotes@gmail.com>
To: OECS@dos.myflorida.com
Elections-1 <Elections-1@sos.mo.gov>
CC: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Mercer, Kalen L. <Kalen.Mercer@dos.myflorida.com>
DivElections <DivElections@dos.myflorida.com>
SOSMain <sosmain@sos.mo.gov>
Date: 3/2/2023 3:07:46 PM
Subject: Two sets of records involving FL and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Florida and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

These matches were detected by citizen group Missouri Canvassers. I concur with the sensibility of the matches and I am relaying their report to you.

Please let me know you have received this email.

MO 73608029
DECKER, LOU ANNE
[redacted]
23 HAVEN VIEW DR ST LOUIS MO 63141 ST. LOUIS
voter-history: 2020 General Election Voted
-- and --
FL MAN 119130457
DECKER, LOUANNE
[redacted]
15903 BAYCROSS DR BRADENTON 34202
voter-history: MAN 119130457 11/03/2020 GEN E
-- detected by NCOA --
LOU ANNE DECKER
ncoa-from: 23 HAVEN VIEW DR ST LOUIS MO 63141 ST. LOUIS
ncoa-to: 15903 BAYCROSS DR LAKEWOOD RANCH FL 34202-2015 MANATEE
ncoa-date: 03/01/2021
-- other info --
[redacted]f2f89426-4f17-479f-9ac1-66d14f7961de?obtained_at=2021-11-17
[redacted]bdea1a81-60d9-4d40-b79d-ed70d9290e8d?obtained_at=2022-11-01

MO ANDREW 751581241
REENTS, TAYLOR EXIE
[redacted]
voter-history: 2020 General Election Voted
-- and --
FL SAR 127729190
REENTS, TAYLOR EXIE
[redacted]
voter-history: SAR 127729190 11/03/2020 GEN E
-- other info --

AMERICAN OVERSIGHT

There is exactly 1 Taylor Reents in the entire FL voter roll, voted or not, of any age with any middle name.
There is exactly 1 Taylor Reents in the entire MO voter roll, voted or not, of any age with any middle name.
Thre are only 3 in the entire VoteRef database of 30 states, all 3 with the same DOB and middle name.
That these have full middle name match and full DOB match indicates they are very likely the same person.
[redacted]fc7d8bfb-1737-4c7d-a454-fc6a9463adc6?obtained_at=2021-11-17
[redacted]62c42c2f-3b73-4403-b9ee-4b48623a91ce?obtained_at=2022-11-01

==========

Totes Legit Votes
A citizen election integrity analyst

From: acohen@nased.org
To: acohen@nased.org
Date: 3/2/2023 2:46:20 PM
Subject: Update, 3/2: NASED Call Notes, Next NASED Call 3/10 @ Noon ET, EAC Hearing 3/15, Electoral Count Reform Act Clarity, Presentations from the Conference, House Admin Hearings, Updated NASED Policy Document, and more!
Attachments: NASED Call 2.24.23.docx
Keller_Winter 2023.pdf
NASED Administrative Policies_Revised 2.28.23.pdf
2023 WorkElections Update.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good afternoon, everyone!

- NASED Call:
  - Attached please find the notes from last week's call. I've included links to some of the legislation in different states that we discussed.
  - Our next call will be **next Friday, March 10 at noon ET**. Nobody complained, so we'll plan on doing a WebEx again. I'll send the link next week.
- EAC:
  - The EAC noticed a hearing today on voter registration list maintenance. The hearing will take place on Wednesday, March 15 at 1pm ET. It will livestream.
- Electoral Count Reform Act:
  - A member raised a question at the conference about the Electoral Count Reform Act (see page 775), which was included in the omnibus budget in December. The law states that the certificate of ascertainment shall "contain at least one security feature, as determined by the State, for purposes of verifying the authenticity of such certificate." The state that raised this wanted to know if there was any clarity on what that security feature should be. I reached out to Senator Klobuchar's staff and Senator Manchin's staff and both advised that the drafters did not have anything specific in mind here, and that the exact security feature is up to the state.
- Conference Wrap Up:
  - I am adding presentations to our website as I get approval from speakers.
  - John Keller from the Department of Justice asked that I share the attached slides with our members directly and not post them.
- Congress:
  - The US House Committee on House Administration, which has jurisdiction over elections, will hold a hearing on Friday, March 10 at 9am ET, "2022 Midterms Look Back Series: Successes in the 2022 Midterm Elections." Witnesses TBD. The hearing will livestream.
    - From the Committee staff: *On the whole, election administration in America is successful. There are multiple ways to vote but one goal of ensuring every interested, eligible American citizen has an opportunity to vote and for their ballot to be counted according to law. The sky isn't falling, and we've learned lessons from the past, preventing systemic voter suppression on the basis of race, sex, etc., today. And, when we've identified places for improvement, it has been the States that have been successful at implementing those improvements (e.g., Florida, Georgia, Ohio, etc.), pushing the "gold standard" higher and higher. We should promote this sort of information sharing between the States through efforts like the American Confidence in Elections Act, which promotes election integrity improvements without mandating them from D.C.*
  - House Admin will hold a hearing later in March (date/time TBD) on Election Observer Access, which I'm told will cover both foreign and domestic election observer access.
- Misc:
  - WorkElections, a project of the Fair Elections Center that helped recruit election workers in2020 and 2022, provided the attached update on their work for 2023.
  - The National Institute of Standards and Technology (NIST) published two common data formats that may be of interest to you, your nerdier staff, or your private sector partners:

AMERICAN OVERSIGHT

        - The Micro Common Data Format
        - The Ballot Definition Common Data Format
- NASED Business:
    - I forgot to mention a few items of NASED business that came out of the conference in my email last week.
        - The members in attendance unanimously approved our FY23 budget, which includes hiring a PT employee and includes paying for DeleteMe as an optional benefit for members in good standing. More to come on both, but very excited about adding to the NASED team!
        - At the NASED Executive Board meeting before the conference, the NASED Executive Board unanimously approved the Investment Policies recommended by the NASED Finance Committee. The full NASED policy document is attached.

I think that's it for today!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Direct: 202-434-8972
Follow us on Twitter @NASEDorg!

The contents of this message, together with any attachments, are confidential and intended only for the use of the individual or entity to which they are addressed. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this message, or any attachment, is strictly prohibited. If you have received this message in error, please notify the original sender immediately by email and delete this message, along with any attachments, from your computer.

--
You received this message because you are subscribed to the Google Groups "All Communciations" group.
To unsubscribe from this group and stop receiving emails from it, send an email to allcomms+unsubscribe@nased.org.

NASED Biweekly Call
Friday, February 24, 2023

RI: Amy included our request for notices/mailings in her email. We're trying to revamp/improve ours, so if anyone has anything to share, please send them our way.

NC: We recently learned about a blog post from the North Carolina Election Integrity Team focusing on the EAC's college poll worker recruitment program that they just got $1M for. People are claiming it's an effort to brainwash college students.
Amy: It's worth noting that the college poll worker recruitment program was included in the original Help America Vote Act, this is just the first time its gotten any money.

NV: Does anyone include first responders in their UOCAVA provisions? We're thinking about firefighters, especially, given the kinds of fires we've had recently.
MS: Yes, we do. (Presentation from NASS 2021 Summer Conference)
NE: We have it. We stole the language from Mississippi. (Statutes 1 and 2)
WV: We have it. (statute)
CO: Us too!
NJ: We're thinking about this, too, and the list I have adds AL, CA, NH, NM, NY, OK, and VA.
NY: New York has a special ballot provision, but the first responder ballot cannot be delivered electronically in the way UOCAVA are.

NV: We're looking at legislation to require realtors to distribute voter registration forms. Has anyone done that?
MS: We did something like this to hand out applications. The Realtors Association loved it, it was part of our 2020 push, so we've continued it. We haven't looked at codifying it, but it's been a successful program for us.

NV: Does anyone have an elections-specific internship program? We're looking to start a DOD SkillBridge program, which takes servicemembers in last 6 months of deployment and sends them to companies like Amazon. DoD pays for it. We're thinking we might be able to hire them as civil investigators.
CO: We have an internship program, but we call them "election fellows" – they're mostly 1Ls and 2Ls. We usually have one or two at any given time. Colorado pays its Fellows $15 a hour. Students can also get academic credit if they're permitted by the school.
OR: We will have our first legal interns this summer through the University of Oregon Law School
NV: SkillBridges often focus on legal programs, EMTs, or other skilled areas.
NC: North Carolina has legal externs typically through Duke Law.

NE: We are seeing some push back from the EAC grants team on projects that we've typically seen as acceptable security projects. It seems like this is coming from the EAC Acting General Counsel regarding security enhancements under HAVA. We were trying to upgrade our less resourced counties to Windows 10 – we can only use HAVA funds for federal elections. We wanted to do a firewall - they would only let us do that for federal elections. We pay for some Albert sensors using HAVA funds, and we're seeing the writing on the wall for Albert. It seems like we will have to stop everything we've done, because if we can't pay for the whole thing, these local jurisdictions aren't going to be able to afford it.

AMERICAN OVERSIGHT

I raised this with the Commissioners at the conference, and someone on staff (Heather Ford) ran up to me afterwards, but that hasn't materialized yet.
CO: I've made the same point regarding firewalls with Mark Robbins on a recent EAC/NASED Board call. He told me they would follow up with documentation about this in federal grants law/regulation, but I haven't received anything yet. I also raised this issue with Senator Bennet and he's on Rules now, so I'm hoping we can make progress.
NE: We were previously told we could buy Alberts with HAVA funds and now we're not sure or will have to allocate the percentage for federal elections. This could be a big step backwards.
Amy: You may want to consider raising this with Senator Fischer's staff since she is the Ranking Member on Rules now.

AMERICAN OVERSIGHT



DOJ Election Threats Task Force

- DOJ—Public Integrity Section: 202-514-1412
  - John Keller, Principal Deputy Chief
  - Robert Heberle, Deputy Chief; Director, Election Crimes Branch
  - Sean Mulryne, Director of Litigation and Enforcement, Election Crimes Branch
- FBI
  - ECCs (Election Crime Coordinators)

AMERICAN OVERSIGHT

Reporting

Today Te
the miss
petition
where h
feeling a
Ted we k
name, a

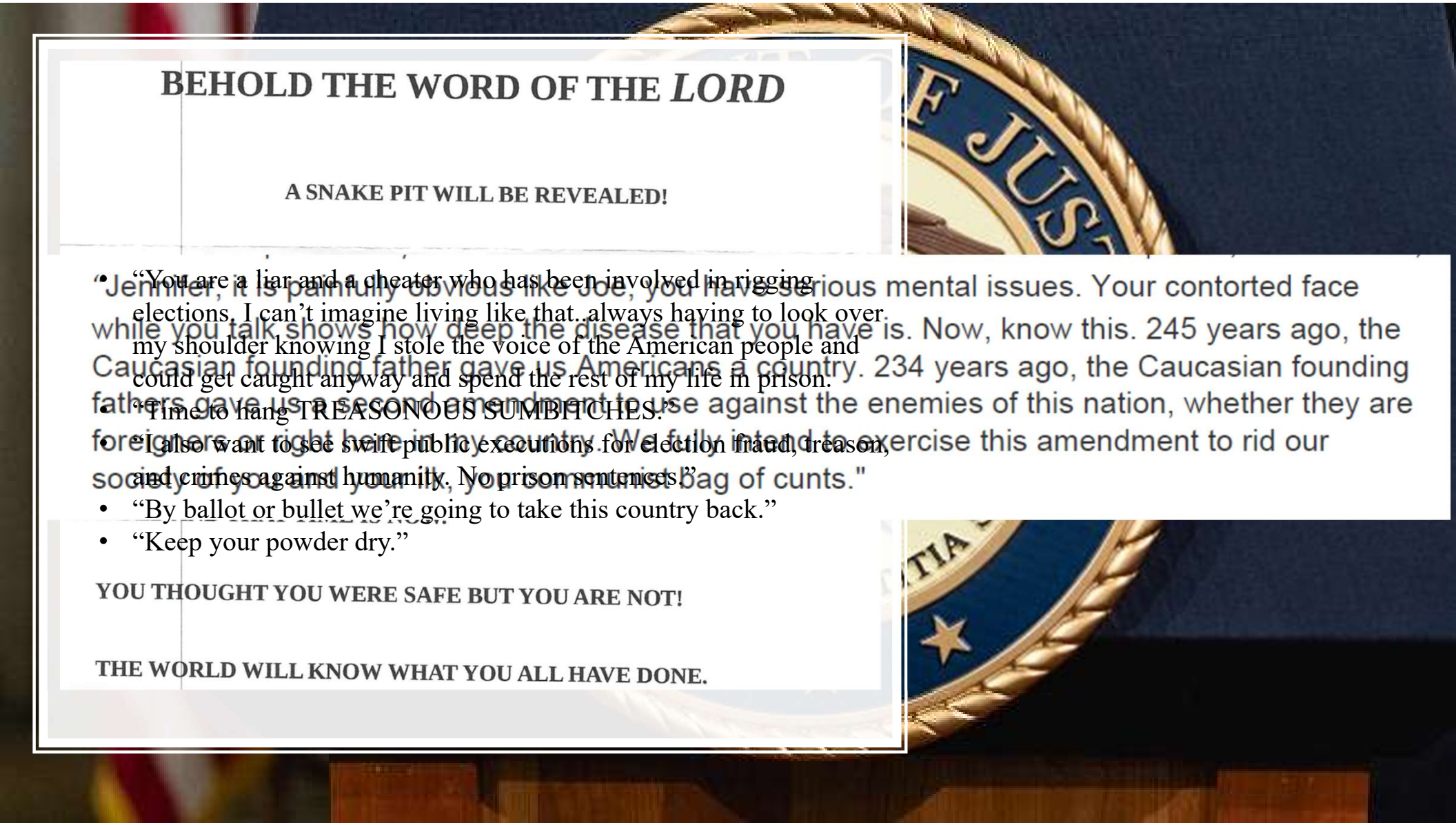
n about
ng
d a call
am
ng with
ow his

Election Crimes Coordinators by Field Office

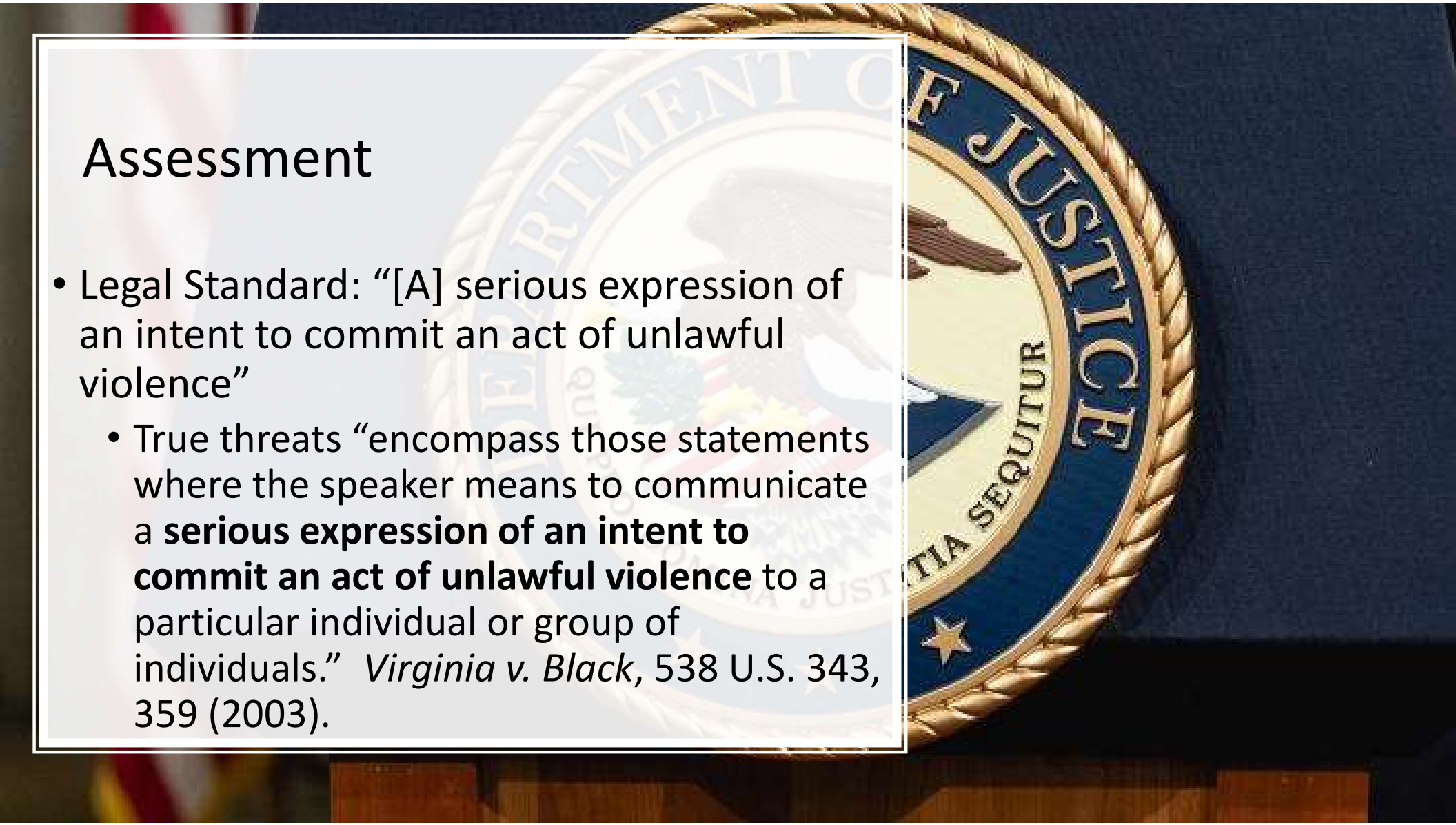
updated 7/29/2022

Field Office	Name	Desk Phone	Bureau Smartphone	Email
Albany (AL)	SA Chris Murphy	518-431-7452	518-764-8838	crmurphy@fbi.gov
	IA Jaime Lugas	518-431-4893	202-440-0236	jlugas2@fbi.gov
	IA Katie M. Miller	518-431-7374	518-414-4518	kmmiller2@fbi.gov
Albuquerque (AQ)	SA Craig Monroney	505-438-5561	410-365-3112	ccmonroney@fbi.gov
	SA Christopher Carlson		505-681-3156	cbcarlson2@fbi.gov
	IA Donald Metzmeier	505-889-1347	505-206-3072	dmetzmeier@fbi.gov
Anchorage (AN)	SA Rory Johnson	907-265-8522	808-284-1782	rbjohnson@fbi.gov
	IA Brian Casey	907-265-8122	907-351-4798	bcasey@fbi.gov
Atlanta (AT)	SA Kimberly Spell-Fowler	770-216-3363	404-922-1401	kspellfowler@fbi.gov
	SA Kelly Gray	770-216-3153	202-579-7076	kfgray@fbi.gov
	IA Matthew Vaveris		703-215-7217	mvaveris@fbi.gov
Baltimore (BA)	SA Greg Mrozek (Delaware)	302-594-4315	302-218-8089	gsmrozek@fbi.gov
	SA Chris Branton (Maryland)		410-310-1577	cgbranton@fbi.gov
	IA Jody Zaruba (Maryland)	410-277-6714	410-200-5659	jezaruba@fbi.gov
	IA Le'Verne Cecere (Delaware)	302-594-4345	443-759-0989	ljcecere@fbi.gov
Birmingham (BH)	SA Stephen Hudgens	205-326-1012	915-472-4959	skhudgens@fbi.gov
	SA Darius Hill		205-533-0975	dhill3@fbi.gov
	IA Stacie Prince	205-279-1519	205-388-4879	sgprince@fbi.gov
Boston (BS)	SA Leah Ferrara	857-386-2401	617-721-3813	lferrara@fbi.gov
	IA Caroline Phelan	857-386-2804	571-660-0632	cdphelan@fbi.gov
Buffalo (BF)	SA Adam Penna	928-314-9631	201-259-6801	apenna@fbi.gov
	IA Lauren Lobur	716-843-5267	716-352-0954	llobur@fbi.gov
Charlotte (CE)	SA James Kaylor	919-854-5859	704-942-8968	jmkaylor@fbi.gov
	IA Jeannine Merritt	704-672-6504	704-604-5869	jamerritt@fbi.gov

AMERICAN OVERSIGHT



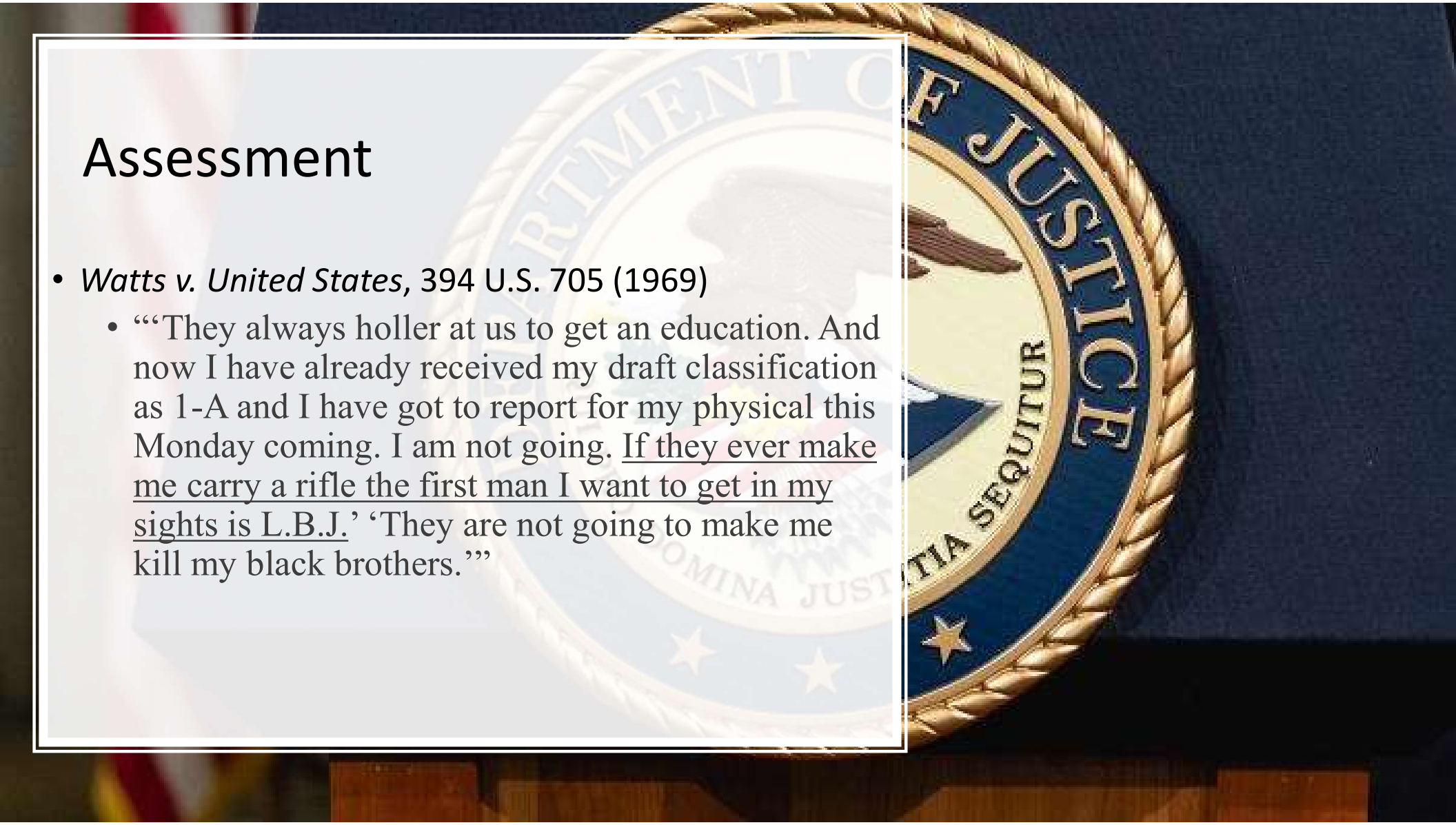
- "You are a liar and a cheater who has been involved in rigging elections. I can't imagine living like that..always having to look over my shoulder knowing I stole the voice of the American people and could get caught anyway and spend the rest of my life in prison."
- "Time to hang TREASONOUS SUMBITCHES."
- "I also want to see swift public executions for election fraud, treason, and crimes against humanity. No prison sentences."
- "By ballot or bullet we're going to take this country back."
- "Keep your powder dry."



Assessment

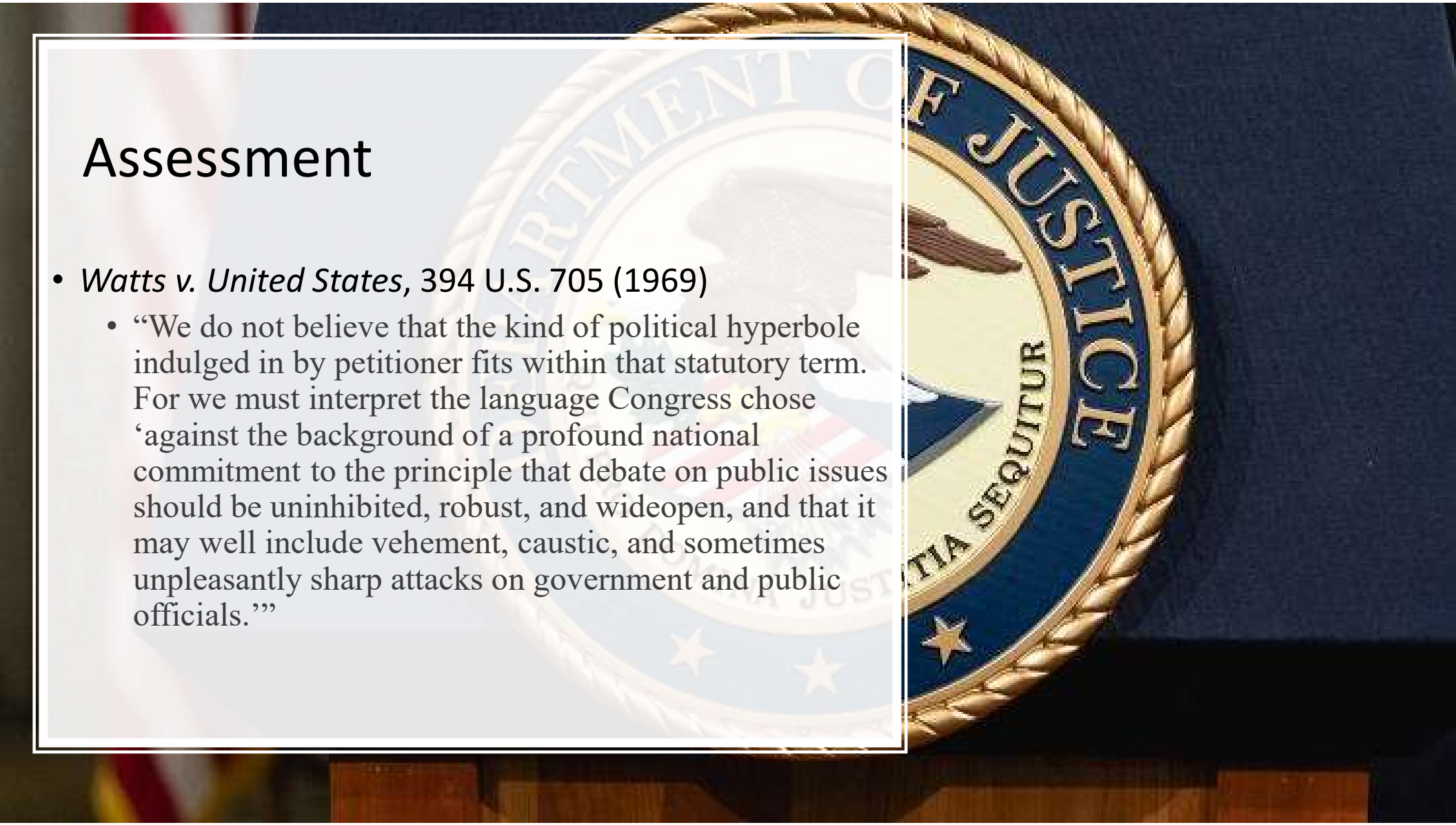
- Legal Standard: "[A] serious expression of an intent to commit an act of unlawful violence"
  - True threats "encompass those statements where the speaker means to communicate a **serious expression of an intent to commit an act of unlawful violence** to a particular individual or group of individuals." *Virginia v. Black*, 538 U.S. 343, 359 (2003).

AMERICAN OVERSIGHT



Assessment

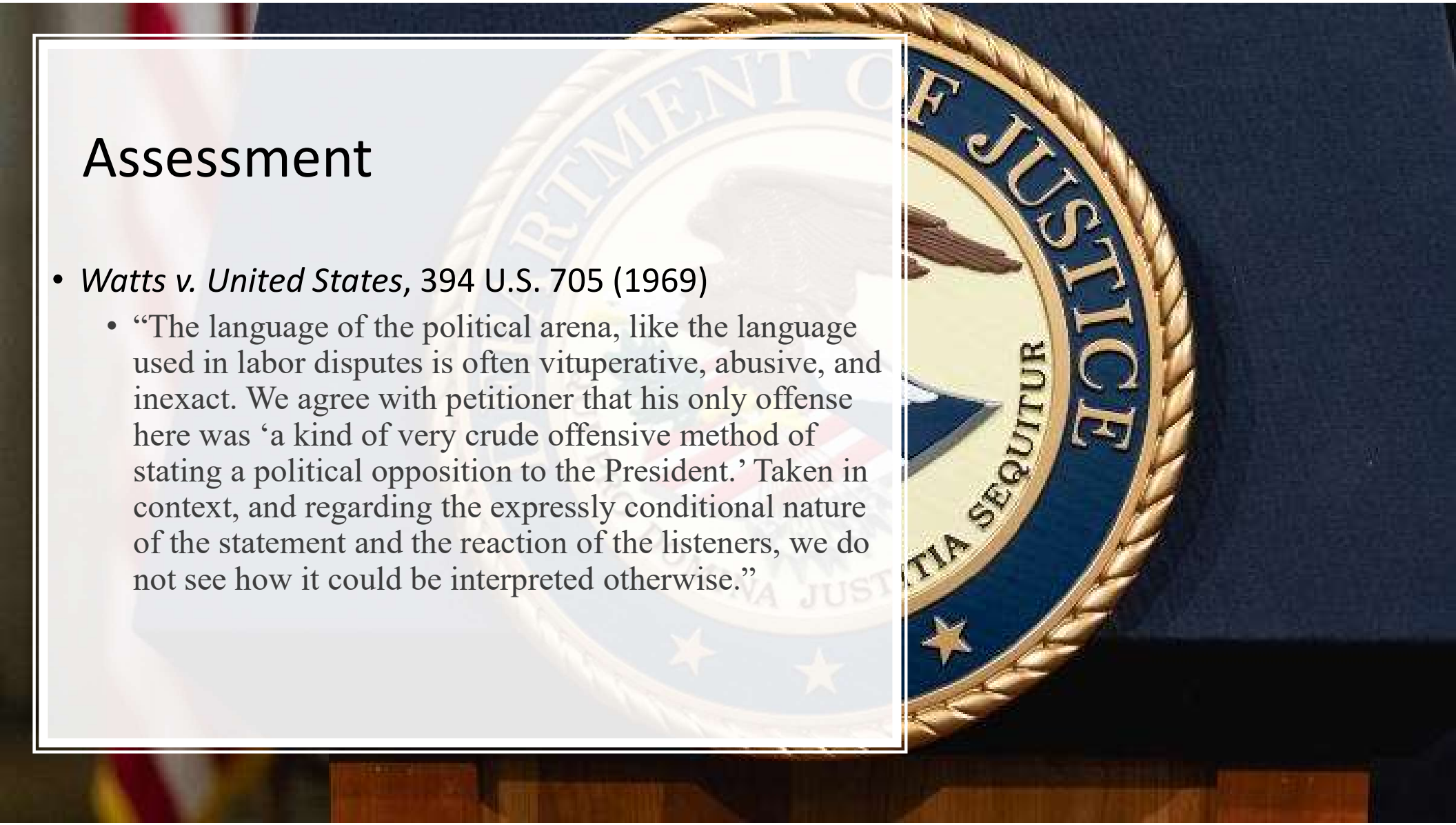
- *Watts v. United States*, 394 U.S. 705 (1969)
  - "'They always holler at us to get an education. And now I have already received my draft classification as 1-A and I have got to report for my physical this Monday coming. I am not going. If they ever make me carry a rifle the first man I want to get in my sights is L.B.J.' 'They are not going to make me kill my black brothers.'"



Assessment

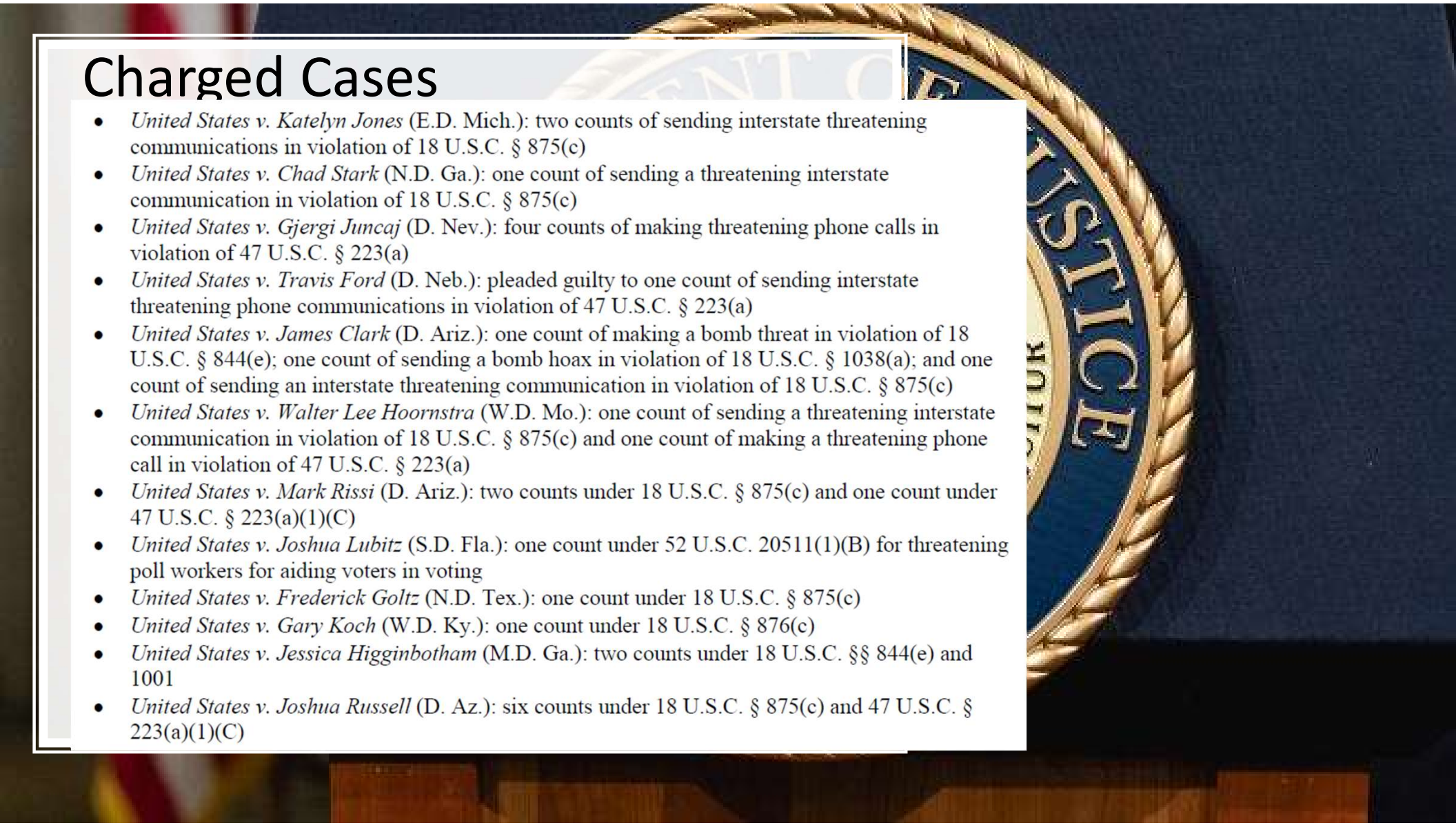
- *Watts v. United States*, 394 U.S. 705 (1969)
  - "We do not believe that the kind of political hyperbole indulged in by petitioner fits within that statutory term. For we must interpret the language Congress chose 'against the background of a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wideopen, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials.'"

AMERICAN OVERSIGHT



Assessment

- *Watts v. United States*, 394 U.S. 705 (1969)
  - "The language of the political arena, like the language used in labor disputes is often vituperative, abusive, and inexact. We agree with petitioner that his only offense here was 'a kind of very crude offensive method of stating a political opposition to the President.' Taken in context, and regarding the expressly conditional nature of the statement and the reaction of the listeners, we do not see how it could be interpreted otherwise."



Charged Cases

- *United States v. Katelyn Jones* (E.D. Mich.): two counts of sending interstate threatening communications in violation of 18 U.S.C. § 875(c)
- *United States v. Chad Stark* (N.D. Ga.): one count of sending a threatening interstate communication in violation of 18 U.S.C. § 875(c)
- *United States v. Gjergi Juncaj* (D. Nev.): four counts of making threatening phone calls in violation of 47 U.S.C. § 223(a)
- *United States v. Travis Ford* (D. Neb.): pleaded guilty to one count of sending interstate threatening phone communications in violation of 47 U.S.C. § 223(a)
- *United States v. James Clark* (D. Ariz.): one count of making a bomb threat in violation of 18 U.S.C. § 844(e); one count of sending a bomb hoax in violation of 18 U.S.C. § 1038(a); and one count of sending an interstate threatening communication in violation of 18 U.S.C. § 875(c)
- *United States v. Walter Lee Hoornstra* (W.D. Mo.): one count of sending a threatening interstate communication in violation of 18 U.S.C. § 875(c) and one count of making a threatening phone call in violation of 47 U.S.C. § 223(a)
- *United States v. Mark Rissi* (D. Ariz.): two counts under 18 U.S.C. § 875(c) and one count under 47 U.S.C. § 223(a)(1)(C)
- *United States v. Joshua Lubitz* (S.D. Fla.): one count under 52 U.S.C. 20511(1)(B) for threatening poll workers for aiding voters in voting
- *United States v. Frederick Goltz* (N.D. Tex.): one count under 18 U.S.C. § 875(c)
- *United States v. Gary Koch* (W.D. Ky.): one count under 18 U.S.C. § 876(c)
- *United States v. Jessica Higginbotham* (M.D. Ga.): two counts under 18 U.S.C. §§ 844(e) and 1001
- *United States v. Joshua Russell* (D. Az.): six counts under 18 U.S.C. § 875(c) and 47 U.S.C. § 223(a)(1)(C)

AMERICAN OVERSIGHT

NATIONAL ASSOCIATION of STATE ELECTION DIRECTORS

NASED Administrative Policies

Financial

The Executive Director must review all contracts with an attorney and other relevant experts as needed. The Executive Director must provide fully executed electronic copies of any contracts to the President, Incoming President, and Treasurer. *Adopted 3/24/18*

In the event a reimbursement is necessary for NASED business expenses, a Reimbursement Request Form must be completed to document where funds were spent and the business purpose. Receipts must be attached. *Adopted 3/24/18*

All reimbursements must be approved by the Executive Director. Executive Director reimbursement requests need to be approved by the Treasurer. Both the Treasurer and the Executive Director must approve any reimbursement greater than $500. *Adopted 3/24/18*

NASED has one credit card that is used by the Executive Director. The Executive Director must notify in writing the President, Incoming President, and Treasurer of any changes to the credit limit. The credit card is used for travel, meeting expenses, and office expenses. Every charge on the credit card must be documented with receipts and the nature of the expense. Personal use of the NASED credit card is prohibited. *Adopted 3/24/18*

All invoices shall be sent to the Executive Director and reviewed to ensure that they are valid and adhere to any previous contract signed, if applicable. Invoices to be paid are entered in the Payment Approval Log to document approval of the invoice along with where the expense should be recorded. Scanned copies of the invoice and associated documentation are saved in digital files. *Adopted 3/24/18*

The Executive Director will process payments for invoices and the credit card at least monthly. The Executive Director must be responsible for entering payments into the financial system and initiating the payment process. *Adopted 3/24/18*

The Executive Director must provide credit card statements to the Treasurer for review. *Adopted 3/24/18*

NASED receives conference and dues payments via check and credit card. Checks must be mailed to the NASED office and deposited by the Executive Director upon receipt and entered into the financial system. Payment received by credit card is deposited automatically into NASED's bank account and automatically updated into the financial system. *Adopted 3/24/18*

The outside accountant must download bank statements for each NASED bank account monthly. The bank statement must be reconciled to the corresponding cash

AMERICAN OVERSIGHT

balances in the financial software. The bank reconciliation must be attached to the bank statement for the month and then reviewed by the Executive Director and Treasurer. *Adopted 3/24/18*

The outside accountant must investigate any uncashed checks greater than four months. *Adopted 3/24/18*

Financial reports must be prepared for each board meeting for review. All NASED members have access to NASED financial records upon request. *Adopted 3/24/18*

Conferences

Non-NASED member speakers invited to present at the NASED conference will not be asked to pay a registration fee. However, those speakers that do not pay a registration fee will not receive a conference packet. Speakers may attend conference social events but will be asked to pay for any social events that require a fee. *Adopted 3/24/18*

Conference attendee lists will be distributed to all registered attendees via email prior to the conference. *Adopted 3/24/18*

No speaker presentations may be distributed or posted on the NASED website without express approval in writing from the speaker. *Adopted 3/24/18*

The Executive Director, at his/her discretion, may permit individuals of value to the field and/or the organization to attend individual conference sessions without registering for the conference. Those individuals who attend without registering will not receive a conference packet. *Adopted 3/24/18*

Members of the media who wish to attend the conference must make that request at least 48 hours before the start of the conference, and will be permitted to attend at no cost, subject to the approval of the Executive Director and subject to availability. Priority will be given to paying attendees. Members of the media must be identified as such and that identification must be visible at all times; those who do not keep their credentials visible at all times may be asked to leave. Members of the media who attend the conference at no cost are responsible for their own meals and breaks. *Adopted 9/17/19*

Starting in 2022, NASED will collocate with the National Association of Secretaries of State (NASS) for summer conferences in even calendar years, unless there is a majority vote of the NASED Executive Board that collocation is not possible or in the best interest of NASED. In odd calendar years, NASED will hold summer conferences at locations chosen by a majority vote of the NASED Executive Board. Winter conferences will always collocate unless there is a majority vote of the NASED Executive Board that collocation is not possible or in the best interest of NASED. When NASED is separate from NASS, NASED will offer an exhibitor area at the conference. *Adopted 1/28/21*

Communications

Any requests made of any NASED member to speak as a representative of NASED must go through the Executive Director and President or the Executive Director must be notified at the time of the request. *Adopted 3/24/18*

AMERICAN OVERSIGHT

If a NASED member, during an interview conducted in the course of doing his or her job, is asked to answer a question on behalf of NASED, that member must notify the Executive Director afterwards. *Adopted 3/24/18*

Executive Board

At its discretion, the Executive Committee may issue statements on issues of concern to the organization. All members of the Executive Committee, including non-voting members, must be given the opportunity to review a statement. Any statement must not be published without the approval of a majority of the voting members of the Executive Committee. *Adopted 7/16/18*

At its discretion, the Executive Committee may respond to public comment on behalf of the organization. All members of the Executive Committee, including non-voting members, must be given the opportunity to review the public comment or voice disagreement with the position. Any comment must not be submitted without the approval of a majority of the voting members of the Executive Committee. *Adopted 7/16/18*

Appointments

Appointments to the Government Coordinating Council

As an organization, NASED appoints four members to the Government Coordinating Council (GCC). Three of those positions are to be held by the NASED President, Incoming President, and Immediate Past President. The fourth position is appointed by the NASED President to a two-year term and may be reappointed for up to two consecutive terms. All NASED appointments must be members in good standing of the organization throughout the term of their appointment. *Adopted 11/10/21*

Of the seven total NASED members who serve on the GCC, at least two must be Chief Election Officials and at least one must represent a state that organizes elections at the municipal level. *Adopted 11/10/21*

Alternate Appointments to the Government Coordinating Council

NASED can appoint Alternates to the Government Coordinating Council (GCC) to serve in the event that one of NASED's four primary appointments to the GCC is unable to attend a meeting. Regional Representatives shall solicit interest annually, and each Region will have one Alternate slot. All NASED appointments must be members in good standing of the organization throughout the term of their appointment. *Adopted 11/10/21*

Appointments

Consistent with the Help America Vote Act (HAVA), NASED makes appointments to the EAC Board of Advisors and the Technical Guidelines Development Committee (TGDC), as well as other advisory boards. All appointments are made by the NASED President. Appointees shall serve a two-year term and may be reappointed for up to two consecutive terms. All NASED appointments must be members in good standing of the organization throughout the term of their appointment. *Adopted 11/10/21*

AMERICAN OVERSIGHT

Code of Conduct for Members, Employees, & Vendors *Adopted 2/28/20*

Prohibited Harassment and Discrimination

NASED is committed to ensuring that all of its Members, Employees, Conference Attendees, and Vendors are able to work with NASED in an environment that is free from harassment and discrimination on the basis of race, religion, creed, color, national origin, citizenship status, ancestry, sex (including pregnancy, childbirth, and related medical conditions), gender (including gender identity and gender expression), sexual orientation, age, physical or mental disability, medical condition, genetic characteristics, marital status, military or veteran status, or any other classification recognized by applicable local, state or federal laws. Accordingly, NASED expects that all Members, Employees, and Vendors adhere to the following Code of Conduct at all times.

Harassment, under this policy, includes verbal or physical conduct that denigrates or shows hostility or aversion toward individual(s) because of one of the aforementioned characteristics that has the purpose or effect of creating an intimidating, hostile, or offensive work environment or has the purpose or effect of unreasonably interfering with someone's relationship with NASED.

Conduct prohibited by this policy is unacceptable on NASED's premises and in any setting where NASED activities are taking place or being discussed, even if outside of NASED's offices, such as in business meetings, business trips, seminars, trainings, business-related events, and social events.

Any person who believes that they have been subject to harassment, or has observed harassment of another, should report the alleged act immediately to Amy Cohen at acohen@nased.org. NASED will undertake an investigation of any complaint. The investigation will be as confidential as possible under the circumstances of the case. Any person who is found to have violated this policy will be subject to appropriate sanctions such as, but not limited to, a loss of privileges to participate in events staged by NASED, termination of employment, or prohibition on conducting business with NASED. The level of sanctions necessary will be those necessary to ensure a harassment free environment.

Prohibited Sexual Harassment

Although harassment for any of the reasons mentioned above is prohibited, sexual harassment is a problem that deserves particular attention. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when: (i) a person's submission to or rejection of such advances, requests, or conduct is made, explicitly or implicitly, a term or condition of association with NASED or enjoyment of the benefits of NASED; (ii) a persons' submission to or rejection of such advances, requests, or conduct is made, explicitly or implicitly, a basis for decisions affecting such person's relationship with NASED; (iii) such conduct has the purpose or effect of substantially interfering with such person's relationship with NASED or creates an intimidating, hostile or offensive environment.

It should be clear from the above definition that sexual harassment not only includes touching or requests for sexual favors but may also involve conduct such as

AMERICAN OVERSIGHT

profanity, sexual innuendos, unwanted comments/compliments about one's body, jokes, pictures, horseplay, or sexually-explicit comments or questions. Such activity is prohibited.

Any person who believes that they have been sexually harassed, or has observed sexual harassment of another, should report the alleged act immediately to Amy Cohen at acohen@nased.org.

NASED will conduct an investigation of any complaint. All efforts will be made to keep the investigation as confidential as possible under the circumstances of the case. The question of whether a particular action or incident is sexual harassment requires a determination based on all the available facts in the matter. If it is determined that the harassment has occurred, the individual who engaged in such harassment will be subject to appropriate sanctions such as, but not limited to, loss of privileges to participate in events staged by NASED, termination of employment, or prohibition on conducting business with NASED.

Retaliation against any person who may allege or formally complain about sexual harassment under this policy, or who assists in any investigation, is prohibited and may result in dismissal. Conversely, a complainant whose allegations are found to be both false and brought with malicious intent will be subject to sanctions.

Prohibited Workplace Conduct

NASED requires Members, Employees, and Vendors to behave appropriately at all times to ensure orderly operations and to provide a suitable environment that protects the interests and safety of all persons associated with NASED. Examples of impermissible conduct that may lead to sanctions are identified below to promote an understanding of what is considered unacceptable conduct. By providing these examples, NASED in no way restricts its discretion to take action against any person engaging in conduct not specifically identified below. It is impossible to provide an exhaustive list.

- Violation of any NASED rule or any action that is detrimental to its business purposes.
- Negligence or any careless or deliberate action which endangers the life or safety of another person.
- Unauthorized possession of dangerous or illegal firearms, weapons, or explosives on NASED's property or at any NASED event.
- Engaging in criminal conduct or acts of violence, or making threats of violence toward anyone on NASED premises or when representing our Company in a business or social setting; fighting, or provoking a fight, on NASED property or at a NASED event; or deliberate or negligent damage of property.
- Threatening or intimidating behavior directed against any person, on or off NASED premises, at any time and for any reason.
- Engaging in an act of sabotage, deliberately or negligently causing the destruction or damage of NASED property, or the property of fellow Members, clients, suppliers, or visitors.
- Theft or unauthorized possession of NASED property or the property of persons associated with NASED.

AMERICAN OVERSIGHT

- Dishonesty, falsification, or misrepresentation on any form or document submitted to NASED.
- Failure to cooperate fully with any investigation.
- Immoral conduct or indecency on NASED property, while representing NASED outside of its offices, or when utilizing NASED-provided services or facilities.
- Any violation of NASED's non-discrimination, non-harassment and non-retaliation policies.

AMERICAN OVERSIGHT

Whistleblower Policy *Adopted 5/28/20*

I. PURPOSES

National Association of State Election Directors, Inc. (the "Organization") is committed to honest, ethical and lawful conduct, full, fair, accurate, timely and transparent disclosure in all public communications, and compliance with applicable laws, rules and regulations. In furtherance of these commitments, all directors, officers, employees, independent contractors, consultants, and volunteers of the Organization (each, a "Covered Person" or "you") must act in accordance with all applicable laws and regulations, and with the policies of the Organization at all times, and assist in ensuring that the Organization conducts its business and affairs accordingly.

This Whistleblower Policy (this "Policy") (a) establishes procedures for the reporting and handling of concerns regarding action or suspected action taken by or within the Organization that is or may be illegal, fraudulent or in violation of any policy of the Organization, as well as any other matter that could cause serious damage to the Organization's reputation (each, a "Concern"), and (b) prohibits retaliation against any Covered Person who reports a Concern in good faith.

By appropriately responding to Concerns, we can better support an environment where compliance is valued and ensure that the Organization is meeting its ethical and legal obligations.

II. WHEN TO RAISE A CONCERN

You are encouraged to disclose to and seek guidance from an appropriate supervisor or manager if you believe any Covered Person or other person associated or doing business with the Organization has engaged, is engaging, or may engage in any illegal or unethical behavior or has violated, or may violate any law, rule, regulation or policy of the Organization. Such reportable activity may include, for example, financial wrongdoing (including circumvention of internal controls or violation of the accounting policies of the Organization), fraud, harassment, or any other illegal, unethical, or proscribed conduct. While Concerns may be submitted at any time, you should report a Concern as soon as reasonably possible after becoming aware of the matter.

III. HOW TO RAISE A CONCERN

Concerns may be submitted either in writing or orally. No specific form is required to be filled out in order to submit a Concern, but you are encouraged to provide as much information and detail as possible so that the Concern can be properly investigated. A Concern may be submitted:

- To the administrator of this Policy (the "Policy Administrator," who is an employee, officer or director of the Organization, as required by law), at acohen@nased.org;
- By discussing it with a supervisor or manager, who will in turn forward the Concern to the Policy Administrator for review where appropriate, or

AMERICAN OVERSIGHT

- In writing (including by e-mail) to the Chair of the Executive Board of the Organization (the "Board"), who will in turn forward the Concern to the Policy Administrator for review where appropriate.

Concerns may be raised anonymously; however, any individual reporting his or her own violation shall not satisfy his/her disclosure obligation hereunder with a Concern raised anonymously. Any individual who is the subject of a Concern is prohibited from participating in any Board or committee deliberations or voting relating to the evaluation of such Concern in accordance with this Policy; provided, that the Board is not prohibited from requesting that such individual present information as background or answer questions at a meeting of the Board prior to the commencement of deliberations or voting relating thereto.

IV. PROCEDURES FOR RECEIVING AND REVIEWING CONCERNS

Any supervisor, manager, or other person receiving a Concern should contact the Policy Administrator (whose contact information is provided in Section III above), who will coordinate further action.

The Policy Administrator will assess each Concern on a preliminary basis to determine to what extent an investigation into the Concern is required, and will direct all aspects of the investigation of any Concern. The Organization will use its best efforts to conduct the review in a confidential manner, so that information will be disclosed only as needed to facilitate review of the investigation materials or otherwise as required by law. You must cooperate as necessary in connection with any such investigation. Any person who does not cooperate in connection with any such investigation may be subject to disciplinary action as determined by the Board. In the event a Concern involves or implicates the Policy Administrator, the Policy Administrator will promptly recuse himself or herself from the investigation and inform the Board in writing. The Board may investigate such Concern or appoint impartial attorneys to investigate the Concern.

V. RECORDS OF CONCERNS AND INVESTIGATION REPORTS

The Policy Administrator will maintain a written record of all Concerns, summarizing in reasonable detail for each Concern: (i) the nature of the Concern (including any specific allegations made and the persons involved); (ii) the date of receipt of the Concern; (iii) the current status of any investigation into the Concern and information about such investigation (including the steps taken in the investigation, any factual findings, and the recommendations for corrective action); and (iv) any final resolution of the Concern. The Policy Administrator will distribute an update of this record to the Chair of the Board in advance of each regularly scheduled meeting thereof.

VI. CONFIDENTIALITY

All Concerns received will be treated confidentially or anonymously, as applicable, to the extent reasonable and practicable under the circumstances.

VII. NO RETALIATION

AMERICAN OVERSIGHT

It is the Organization's policy to encourage the communication of bona fide Concerns relating to the lawful and ethical conduct of the Organization's business. It is also the policy of the Organization to protect those who communicate bona fide Concerns from any retaliation for such reporting. **No adverse employment action or other forms of retaliation (including, without limitation, intimidation, harassment, discrimination, coercion, or otherwise, whether express or implied) may be taken against any Covered Person based on such person having reported in good faith any Concern or assisted in an investigation of, or the fashioning or implementation of any corrective action or response made in connection with, any Concern.** Any person who violates this prohibition against retaliation will be subject to appropriate disciplinary action, which may include termination of employment or other relationship with the Organization.6

VIII. POLICY DISTRIBUTION

A copy of this Policy will be distributed to each Covered Person promptly following the adoption of or any amendments to this Policy, and at such time as a person becomes a Covered Person. This distribution requirement may be satisfied by posting a copy of this Policy on the Organization's website.

IX. POLICY ADOPTION AND OVERSIGHT

The Board is ultimately responsible for providing oversight of the adoption and implementation of, and compliance with, this Policy.

This Whistleblower Policy was adopted by the Board on May 28, 2020.

AMERICAN OVERSIGHT

Document Retention Policy *Adopted 5/28/20*

ARTICLE I

PURPOSE

The purposes of this document retention policy are for National Association of State Election Directors, Inc. (the "Organization") to promote the proper treatment of corporate records of the Organization.

ARTICLE II

POLICY

Section 1. General Guidelines. Records should not be kept if they are no longer needed for the operation of the business or required by law. Unnecessary records should be eliminated from the files. The cost of maintaining records is an expense which can grow unreasonably if good housekeeping is not performed. A mass of records also makes it more difficult to find pertinent records.

From time to time, the Organization may establish retention or destruction policies or schedules for specific categories of records in order to ensure legal compliance, and also to accomplish other objectives, such as preserving intellectual property and cost management. Several categories of documents that warrant special consideration are identified below. While minimum retention periods are established, the retention of the documents identified below and of documents not included in the identified categories should be determined primarily by the application of the general guidelines affecting document retention, as well as the exception for litigation relevant documents and any other pertinent factors.

Section 2. Exception for Litigation Relevant Documents. The Organization expects all officers, directors, and employees to comply fully with any published records retention or destruction policies and schedules, provided that all officers, directors, and employees should note the following general exception to any stated destruction schedule: If you believe, or the Organization informs you, that Organization records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until it is determined that the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records.

Section 3. Minimum Retention Periods for Specific Categories.

(a) Organizational Documents. Organizational records of the Organization, include, but not limited to, the Organization's articles of incorporation, by-laws. Organizational records should be retained permanently. IRS regulations require that the Form 1023 be available for public inspection upon request.

(b) Tax Records. Tax records include, but may not be limited to, documents concerning payroll, expenses, proof of contributions made by donors, accounting procedures, and other documents concerning

AMERICAN OVERSIGHT

the Organization's revenues. Tax records should be retained for at least seven years from the date of filing the applicable return.

(c) Employment Records/Personnel Records. State and federal statutes require the Organization to keep certain recruitment, employment and personnel information. The Organization should also keep personnel files that reflect performance reviews and any complaints brought against the Organization or individual employees under applicable state and federal statutes. The Organization should also keep in the employee's personnel file all final memoranda and correspondence reflecting performance reviews and actions taken by or against personnel. Employment applications should be retained for three years. Retirement and pension records should be kept permanently. Other employment and personnel records should be retained for seven years.

(d) Board and Board Committee Materials. Meeting minutes should be retained in perpetuity in the Organization's minute book. A clean copy of all other Board and Board Committee materials should be kept for no less than three years by the Organization.

(e) Press Releases/Public Filings. The Organization should retain permanent copies of all press releases and publicly filed documents under the theory that the Organization should have its own copy to test the accuracy of any document a member of the public can theoretically produce against the Organization.

(f) Legal Files. Legal counsel should be consulted to determine the retention period of particular documents, but legal documents should generally be maintained for a period of ten years.

(g) Marketing and Sales Documents. The Organization should keep final copies of marketing and sales documents for the same period of time it keeps other corporate files, generally three years. An exception to the three-year policy may be sales invoices, contracts, leases, licenses, and other legal documentation. These documents should be kept for at least three years beyond the life of the agreement.

(h) Development/Intellectual Property and Trade Secrets. Development documents are often subject to intellectual property protection in their final form (e.g., patents and copyrights). The documents detailing the development process are often also of value to the Organization and are protected as a trade secret where the Organization:

AMERICAN OVERSIGHT

(i) derives independent economic value from the secrecy of the information; and
(ii) has taken affirmative steps to keep the information confidential.

The Organization should keep all documents designated as containing trade secret information for at least the life of the trade secret.

(i) Contracts. Final, execution copies of all contracts entered into by the Organization should be retained. The Organization should retain copies of the final contracts for at least three years beyond the life of the agreement, and longer in the case of publicly filed contracts.

(j) Correspondence. Unless correspondence falls under another category listed elsewhere in this policy, correspondence should generally be saved for two years.

(k) Banking and Accounting. Accounts payable ledgers and schedules should be kept for seven years. Bank reconciliations, bank statements, deposit slips and checks (unless for important payments and purchases) should be kept for three years. Any inventories of products, materials, and supplies and any invoices should be kept for seven years.

(l) Insurance. Expired insurance policies, insurance records, accident reports, claims, etc. should be kept permanently.

(m) Audit Records. External audit reports should be kept permanently. Internal audit reports should be kept for three years.

Section 4. Electronic Mail. E-mail that needs to be saved should be either:

(i) printed in hard copy and kept in the appropriate file; or

(ii) downloaded to a computer file and kept electronically or on disk as a separate file.

The retention period depends upon the subject matter of the e-mail, as covered elsewhere in this policy.

AMERICAN OVERSIGHT

Conflict of Interest Policy *Adopted 5/28/20*

Purpose

The purpose of the conflict of interest policy is to protect this tax-exempt organization's National Association of State Election Directors ("NASED") interest when it is contemplating entering into a transaction or arrangement that might benefit the private interest of a, member, officer or director of NASED or might result in a possible excess benefit transaction. This policy is intended to supplement but not replace any applicable state and federal laws governing conflict of interest applicable to nonprofit and charitable organizations.

ARTICLE I
Definitions

1.1 Interested Person

Any director, principal officer, or member of a committee with governing board delegated powers, who has a direct or indirect financial interest, as defined below, is an interested person.

1.2 Financial Interest

A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:

a. An ownership or investment interest in any entity with which NASED has a transaction or arrangement,

b. A compensation arrangement with NASED or with any entity or individual with which NASED has a transaction or arrangement, or

c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which NASED is negotiating a transaction or arrangement.

Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

A financial interest is not necessarily a conflict of interest. Under Article III, Section 2, a person who has a financial interest may have a conflict of interest only if the appropriate governing board or committee decides that a conflict of interest exists.

ARTICLE II
Procedures

2.1 Duty to Disclose

In connection with any actual or possible conflict of interest, an interested person must disclose the existence of the financial interest and be given the opportunity to disclose all material facts

AMERICAN OVERSIGHT

to the directors and members of committees with governing board delegated powers considering the proposed transaction or arrangement.

2.2 Determining Whether a Conflict of Interest Exists

After disclosure of the financial interest and all material facts, and after any discussion with the interested person, he/she shall leave the governing board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

2.3 Procedures for Addressing the Conflict of Interest

a. An interested person may make a presentation at the governing board or committee meeting, but after the presentation, he/she shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.

b. The chairperson of the governing board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.

c. After exercising due diligence, the governing board or committee shall determine whether NASED can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.

d. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the governing board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in NASED's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination it shall make its decision as to whether to enter into the transaction or arrangement.

2.4 Violations of the Conflicts of Interest Policy

a. If the governing board or committee has reasonable cause to believe a member has failed to disclose actual or possible conflicts of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.

b. If, after hearing the member's response and after making further investigation as warranted by the circumstances, the governing board or committee determines the member has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

AMERICAN OVERSIGHT

ARTICLE III
Records of Proceedings

The minutes of the governing board and all committees with board delegated powers shall contain:

a. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the governing board or committee's decision as to whether a conflict of interest in fact existed.

b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

ARTICLE IV
Compensation

a. A voting member of the governing board who receives compensation, directly or indirectly, from NASED for services is precluded from voting on matters pertaining to that member's compensation.

b. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from NASED for services is precluded from voting on matters pertaining to that member's compensation.

c. No voting member of the governing board or any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from NASED, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

ARTICLE V
Annual Statements

Each director, principal officer and member of a committee with governing board delegated powers shall annually sign a statement which affirms such person:

a. Has received a copy of the conflicts of interest policy,

b. Has read and understands the policy,

c. Has agreed to comply with the policy, and

AMERICAN OVERSIGHT

d. Understands NASED is charitable and in order to maintain its federal tax exemption it must engage primarily in activities which accomplish one or more of its tax-exempt purposes.

ARTICLE VI
Periodic Reviews

To ensure NASED operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

a. Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining.

b. Whether partnerships, joint ventures, and arrangements with management organizations conform to NASED's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

ARTICLE VII
Use of Outside Experts

When conducting the periodic reviews as provided for in Article VII, NASED may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the governing board of its responsibility for ensuring periodic reviews are conducted.

AMERICAN OVERSIGHT

NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS CONFLICT OF INTEREST POLICY

DISCLOSURE FORM

The undersigned, as a Board member or officer of National Association of State Election Directors ("NASED"), acknowledges that:

1. he or she has received a copy of NASED's Conflict of Interest Policy (the "Policy");
2. he or she has read and understands the Policy;
3. he or she has agreed to comply with the Policy;
4. he or she understands that NASED was organized for charitable purposes and, in order to maintain its federal tax-exempt status, it must engage primarily in activities which accomplish one or more of its tax-exempt purposes; and
5. the following relationships and interests may present a potential or actual conflict of interest:

(disclosures should address current affiliations, as well as past affiliations for at least the prior two years, and should include all of the following: the undersigned's employer, all corporations (nonprofit and for-profit) of which the undersigned is a board member or officer, and the names of such of the undersigned's Family Members, as defined in the Policy, or business affiliates or any other relationships the undersigned has which the undersigned believes may present a potential conflict)

_____

_____

_____

_____

_____

_____

Name: _____

Title: _____

Signature: _____

Date: _____

AMERICAN OVERSIGHT

Sick and Safe Leave of Absence *Adopted 12/9/20*

The Company will provide employees with ten (10) days of sick and safe leave ("SSLA") per year. Employees will accrue such leave immediately upon hire. Exempt employees do not accrue leave for hours worked beyond a 40-hour workweek.

Sick and safe leave may be used for any of the following purposes:

- An absence resulting from a physical or mental illness, injury, or medical condition of the employee or covered family member.
- An absence resulting from obtaining professional medical diagnosis or care, or preventive medical care, for the employee or covered family member.
- An absence directly related to social or legal services pertaining to stalking, domestic violence, or sexual abuse of the employee or family member, in order to:
  - Seek medical attention for the employee or the employee's family member to recover from physical or psychological injury or disability caused by domestic violence or sexual abuse;
  - Obtain services from a victim services organization;
  - Obtain psychological or other counseling;
  - Temporarily or permanently relocate;
  - Take legal action, including preparing for or participating in any civil or criminal legal proceeding related to or resulting from the domestic violence or sexual abuse; or
  - Take other actions to enhance the physical, psychological, or economic health or safety of the employee or the employee's family member or to enhance the safety of those who associate or work with the employee.

"Family member" is defined to include the following:

- A spouse (including the person identified by an employee as his or her domestic partner), the parents of a spouse, children (including foster children and grandchildren), the spouses of children, parents, brothers and sisters, and the spouses of brothers and sisters.
- A child who lives with an employee and for whom the employee permanently assumes and discharges parental responsibility.
- A person with whom the employee shares or has shared, for not less than the preceding 12 months, a mutual residence and with whom the employee maintains a committed relationship.

Employees must follow these procedures in order to have leave designated as sick and safe leave:

- If the need for leave is foreseeable, the employee must request leave at least 10 days prior to missing work.
- If the reason is not foreseeable, the employee must provide notice of the leave prior to the start of the work shift to be missed.

AMERICAN OVERSIGHT

- In the case of an emergency, the employee shall provide notice prior to the start of the next work shift or within 24 hours of the onset of the emergency, whichever comes first.

For absences of three or more days, the employee must provide a reasonable certification of the reason for the leave.

DC Parental Leave *Adopted 12/9/20*

The Company will provide an employee who is a parent with a total of 24 hours of leave during any 12-month period to attend or participate in a school-related event for his or her child. The leave is unpaid unless the employee elects to substitute available paid leave. Leave must be scheduled 10 calendar days in advance, unless the need to attend the event was not reasonably foreseeable.

For purposes of this requirement, a "parent" includes any of the following:

- The natural mother or father of a child
- A person who has legal custody of a child
- A person who acts as a guardian of a child regardless of whether he or she has been appointed legally as such
- An aunt, uncle, or grandparent of a child
- A person who is married to, or in a domestic partnership with, any of the foregoing individuals

A "school-related event" is an activity sponsored by either a school or an associated organization, such as a parent-teacher association. A school-related event may include a student performance such as a concert, play, or rehearsal; a school sporting game or practice; a meeting with a teacher or counselor; or any similar activity. *A school-related event must involve the parent's child directly either as participant or subject, and not merely as a spectator.*

The Company may deny a request for parental leave if it would disrupt business and make the achievement of production or service delivery unusually difficult.

Universal Paid Leave *Adopted 12/9/20*

D.C. provides the following government-administered paid leave to D.C. employees:

- Up to 8 weeks per year to bond with a new child.
- Up to 6 weeks per year to care for a family member with a serious health condition.
- Up to 2 weeks per year to care for the employee's own serious health condition.

AMERICAN OVERSIGHT

To the extent practicable, employees must provide 10 days' advanced written notice of the need to take paid-leave. If the need for leave is unforeseeable, employees must provide oral or written notification before the start of the work shift for which paid leave is being used. In the case of an emergency, the employee, or another individual on behalf of the employee, must provide notification of the need for leave within 48 hours of the emergency occurring.

Upon the occurrence of a qualifying event, employees may file a claim for paid leave benefits with the Department of Employment Services.

Accommodations for Pregnant Employees *Adopted 12/9/20*

The Company will provide reasonable accommodations for workers whose ability to perform the functions of a job are limited by pregnancy, childbirth, a related medical condition, pre-birth complication, or breastfeeding, including time off to recover from childbirth. Reasonable accommodations may include:

- More frequent or longer breaks
- Time off to recover from childbirth
- The acquisition or modification of equipment or seating
- A temporary transfer to a less strenuous or less hazardous position or other job restructuring such as providing light duty or a modified work schedule
- Having the employee refrain from heavy lifting
- Relocating the employee's work area
- Providing private non-bathroom space for expressing breast milk

An accommodation is not reasonable if it would cause an undue hardship in the operation of the Company's business. "Undue hardship" is defined as any action that requires significant difficulty in the operation of the Company's business or significant expense to the Company when considered in relation to factors such as size of the business, its financial resources, and the nature and structure of the operation.

Employees will be required to provide a certification from a health care provider informing the Company of the medical advisability of a reasonable accommodation, to the same extent a certification is required for other temporary impairments.

Hiring and Benefits *Adopted 12/9/20*

The NASED Executive Director's job description is developed by the Executive Board. Hiring decisions for this position are made by the Executive Board. The NASED Executive Director reports to the Executive Board.

The NASED President must approve time-off requests for the Executive Director in writing.

AMERICAN OVERSIGHT

The Executive Director's annual review, done on the hire date anniversary, is conducted by the Executive Board.

AMERICAN OVERSIGHT

Investment Policy *Adopted 2/15/23*

Investment Objective

The overall investment objective of the Organization is to maximize the return on invested assets while minimizing risk and expenses. This is done through prudent investing and planning, as well as through the maintenance of a diversified portfolio.

General Provisions

- All transactions shall be for the sole benefit of the Organization.
- The Executive Board shall conduct a review of this policy at least every four years starting in 2027.
- The Executive Board will operate the Organization's investment program in compliance with all applicable state, federal and local laws and regulations concerning management of investment assets.
- Investments shall be diversified to maximize return while minimizing risk.
- Any amount exceeding 12 months of operating expenses in the NASED checking accounts shall be transferred to the NASED investment account at a date and time chosen by the Finance Committee.

Delegation of Responsibility

The Executive Board has a direct oversight role regarding all decisions that affect NASED's institutional funds. The Board has delegated supervisory responsibility for the management of institutional funds to the Finance Committee. Specific responsibilities of the various bodies and individuals responsible for the management of institutional funds are set forth below:

Responsibilities of The Board

The Board shall ensure that its fiduciary responsibilities concerning the proper management of NASED's institutional funds are fulfilled through appropriate investment structure, internal and external management, and portfolio performance consistent with all policies and procedures. Based on the advice and recommendations of the Finance Committee, the Board shall approve investment policies and objectives that reflect the long-term investment-risk orientation of the Organization.

Responsibilities of the Finance Committee

The Finance Committee is accountable to the NASED Executive Board. Members of the Finance Committee are not held accountable for less than desirable outcomes,

AMERICAN OVERSIGHT

rather for adherence to procedural prudence, or the process by which decisions are made in respect to investment assets. In consideration of the foregoing, the Committee is responsible for the development, recommendation, implementation and maintenance of all policies relative to NASED's institutional funds and shall:

1. Develop and/or propose policy recommendations to the Board with regard to the management of all institutional funds.
2. Determine that institutional funds are prudently and effectively managed with the assistance of management and any necessary financial planners and/or outside professionals.
3. Monitor and evaluate the performance of all those responsible for the management of institutional funds.
4. Recommend the retention and/or dismissal of financial planners and/or other outside professionals.
5. Receive and review reports from management, financial planners, and/or other outside professionals.
6. Periodically meet with management, financial planners, and/or other outside professionals.
7. Regularly evaluate whether this policy, investment activities, and risk management controls and processes continue to be consistent with meeting the goals and objectives set for the management of institutional funds; and,
8. Determine the Organization's risk tolerance and investment horizon and communicate these to the appropriate parties.
9. Report on a regular basis to the NASED Executive Board on the investment outcomes.

Responsibilities of Management

Management shall be responsible for the day-to-day administration and implementation of policies established by the Board and/or the Finance Committee concerning the management of institutional funds. Management shall also be the primary liaison between any investment consultants and/or other outside professionals that may be retained to assist in the management of such funds. Specifically, management shall:

- Oversee the day-to-day operational investment activities of all institutional funds subject to policies established by the Board and/or the Finance Committee.
- Engage with any necessary outside service providers such as financial planners or consultants.
- Ensure that the service providers adhere to the terms and conditions of their contracts, have no material conflicts of interest with NASED, and employ performance monitoring systems sufficient to provide the Finance Committee with timely, accurate, and useful advice.

AMERICAN OVERSIGHT

- Regularly meet with any outside service providers to evaluate and assess compliance with investment guidelines, performance, outlook, and investment strategies.
- Monitor asset allocation in accordance with approved asset allocation policies and tend to all other matters deemed to be consistent with respect to prudent management of institutional funds.
- Comply with official accounting and auditing guidelines regarding due diligence and ongoing monitoring of investments.
- Prepare and issue periodic status reports to the Board and/or the Finance Committee.

AMERICAN OVERSIGHT

General Investment Guidelines

- A copy of this Investment Policy shall be provided to all Investment Managers or Financial Planners.
- The Organization is a tax-exempt organization as described in section 501(c)(3) of the Internal Revenue Code. This tax-exempt status should be taken into consideration when making Organization investments.
- Permitted investments include: Cash and cash equivalents or marketable securities including equities and fixed income securities.
- The following transactions are prohibited: International emerging markets, crypto or digital currencies, NFTs, and high-risk investment options, including short sales and margin transactions.

Diversification

- The Organization will maintain a reasonable diversification of investment assets between asset classes and investment categories at all times.
- Investments within the investment portfolio should be readily marketable.
- The investment portfolio should not be a blind pool; each investment must be available for review.

Withdrawal

In consultation with the Finance Committee, the Executive Board may vote to withdraw operating funds from the investment account in the event a majority of the Board deems it necessary.

AMERICAN OVERSIGHT

2023 Update

What is WorkElections?

WorkElections.org is a website created by the nonpartisan, non-profit Fair Elections Center to centralize poll worker requirements and applications for jurisdictions around the country.

The website has info for over 5,000 jurisdictions nationwide, making it easy for the public to learn how they can become poll workers in their area. WorkElections is a one-stop shop containing simplified information for prospective poll workers who may not know where or how to apply.

Our Goals

- Ensuring that election officials are able to recruit sufficient staff to administer elections and that no polling places are closed due to a lack of workers.
- Helping election officials to recruit a new generation of poll workers and to diversify their pool of poll workers to better reflect the voters they serve.

Our Work in 2022

- Conducted outreach to thousands of election offices across the country to gather up-to-date information about poll worker recruitment and application links. This entailed over 2,400 phone calls and 4,500 emails to election offices.
- Provided database for use by Power the Polls, of which Fair Election Center is a founding partner. In 2022, Power the Polls engaged over 275,000 potential poll workers.
- Shared lists of Power the Polls signups with election offices that were in need of additional applicants in the advance of the November 2022 election.

How You Can Help

- Remind local election officials in your state about this resource.
- Encourage local election officials to share updates to poll worker information or applications so we can keep their jurisdictions' WorkElections pages up-to-date.
- Notify us regarding poll worker needs in your state (e.g. staff shortages or specific language/technology skills in high demand).
- Develop a statewide online poll worker application to streamline the recruitment process.

Looking Forward

WorkElections.org and Power the Polls stand ready to assist election officials with meeting poll worker needs for the 2023 elections. We aim to deepen our collaboration with election officials in advance of the 2024 election cycle.

A Project of FAIR ELECTIONS CENTER

Contact Us

Please email
ryan@fairelectionscenter.org
with any questions.

MO-SOS-23-0911-A-000155

AMERICAN OVERSIGHT

From: Nodaway County <Nodaway.County@sos.mo.gov>
To: Straub, Dee Dee <deedee.straub@sos.mo.gov>
Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 3/2/2023 10:06:19 AM
Subject: Re: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

In looking at it with fresh eyes this morning....we looked at our audit log and it looks like we had followed up with him and he confirmed that he does live here. However, I think he has a TX driver's license.

I'm definitely interested in feedback on what I need to do to prevent this fromhappening again and also if I need to do anything on my end for this particular issue.

Thank you-

Melinda

From: Straub, Dee Dee
Sent: Thursday, March2, 2023 7:13:03AM
To: Nodaway County
Subject: RE: Potential Double voter in2020 GE in Nodaway County, MO and Johnson County, TX

Good Morning, Melinda---

Chrissy will have to take a look at it and decide.
Thank you!!
Dee Dee

From: Nodaway County <Nodaway.County@sos.mo.gov>
Sent: Wednesday, March 1, 2023 5:52 PM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Pauley, Scott <Scott.Pauley@sos.mo.gov>; Straub, Dee Dee <deedee.straub@sos.mo.gov>; Elections-1 <Elections-1@sos.mo.gov>
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton
Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March 1, 2023 4:12 PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

AMERICAN OVERSIGHT

I am bringing to your attention what appears to be a person who double voted in the states of Texas and Missouri in the 2020 General Election.

See TX statutes: Sec. 64.012(A)(1), Sec. 64.012(A)(2), Sec. 64.012(A)(5), Sec. 276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON
dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]
dor: 08/16/2016
1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]
dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted] 1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

AMERICAN OVERSIGHT

Thank you for your time and investigation into this matter.

Please confirm receipt of this email.

All The Best,
Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

From: Nodaway County <Nodaway.County@sos.mo.gov>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Pauley, Scott <Scott.Pauley@sos.mo.gov>
Straub, Dee Dee <deedee.straub@sos.mo.gov>
Elections-1 <Elections-1@sos.mo.gov>
Date: 3/1/2023 5:51:59 PM
Subject: Fw: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX
Attachments: Dobson TX Info.pdf

I'm unsure who I should send this to, so I've sent it to several of you.

Are you able to advise me on what, if anything, I should do with this email?

Thank you-

Melinda Patton
Nodaway County Clerk

From: Ian Camacho <ian.c.camacho@gmail.com>
Sent: Wednesday, March1, 2023 4:12PM
To: vote@johnsoncountytx.org; nodclerk@gmail.com; Nodaway County; Nodaway County
Cc: SOSMain; Elections-1
Subject: Potential Double voter in 2020 GE in Nodaway County, MO and Johnson County, TX

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Nodaway County, MO and Johnson County, TX Elections Divisions,

I am bringing to your attention what appears to be a person who double voted in the states of Texas and Missouri in the 2020 General Election.

See TX statutes: Sec64.012(A)(1), Sec.64.012(A)(2), Sec.64.012(A)(5), Sec.276.013 (A)(1)(3), & Sec. 276.013 (A)(1)(8)

More specifically, it appears that this person voted in both Nodaway County, MO and Johnson County, TX in the 2020 General Election.

This address and vote was detected by voter registration, voting records, and the NCOA.

AARON JOSEPH DOBSON
dob: [redacted]

MO 44750439
AARON JOSEPH DOBSON
dob: [redacted]
dor: 08/16/2016

AMERICAN OVERSIGHT

1207 PARKDALE RD MARYVILLE MO 64468
2020 General Election

-- and --

TX JOHNSON 2150436859
DOBSON, AARON JOSEPH
dob: [redacted]
dor: 11/06/2018
2580 CR 425 CLEBURNE TX 76031
11/3/2020 GE EV

-- detected by NCOA --
AARON JOSEPH DOBSON
1207 PARKDALE RD MARYVILLE MO 64468
2580 COUNTY ROAD 425 CLEBURNE TX 76031-8804 JOHNSON
07/01/2018

Potential double voting issue aside, the 2016 MO registration would have been ineligible due to the later 2018 TX registration, and thus the MO 2020 ballot was potentially illegally cast due to the later TX registration.

Attached is one registration and voting document pertaining to Mr. Dobson in TX (unable to pull up MO as I lack his social security number).

An independent third party site voteref.com confirms the addresses, registration dates, and the general elections in which he voted in Texas and Missouri.

The dates that the voter records were obtained are shown on the website.

[redacted] f2218-b677-44ad-a096-badc85dd2194?obtained_at=2021-11-17 (MO)

[redacted]1a4a60a-edee-4047-8b38-548c73aefe60?obtained_at=2022-01-26 (TX)

Thank you for your time and investigation into this matter.
Please confirm receipt of this email.

All The Best,
Ian Camacho
310 775 3540

AMERICAN OVERSIGHT

TEXAS SECRETARY OF STATE

MY VOTER PORTAL
TEXAS ELECTIONET ADMINISTRATION SYSTEM

Voter Information

Name: AARON JOSEPH DOBSON
Address: 2580 CR 425
CLEBURNE TX 76031 - 8804
Gender: MALE
Valid From: 01/01/2022
Effective Date of Registration: 11/06/2018
Voter Status: ACTIVE
County: JOHNSON
Precinct: 21
VUID: 2150436859

Change your Address

Upcoming Elections (Select Election for available polling information)

11/07/2023--2023 NOVEMBER 7TH CONSTITUTIONAL AMENDMENT

***Eligibility is determined by Effective Date of Registration (Must be on or before Election Day)

Please Note: Polling places are subject to change. Always check your designated polling place location via this website or by contacting your county prior to going to vote.

ADDITIONAL QUESTIONS and FAQ

Note: Any questions now that you see your voter registration status? On Suspense? Don't live at that address anymore? Not sure what to do next? Check out our FAQ.

Back

AMERICAN OVERSIGHT

From: Peters, Chrissy
To: Winn, Jody <Jody.Winn@sos.mo.gov>
Date: 3/1/2023 11:25:48 AM
Subject: RE: Four sets of records involving FL and MO that need additional inspection.

Do not click on these links. Thanks

Chrissy Peters | Director of Elections
Missouri Secretary of State Jay Ashcroft
600 West Main Street | Jefferson City, MO 65102
Phone: (573) 526-3986 | 1-800-669-8683

Missouri Secretary of State
Elections

From: Elections-1 <Elections-1@sos.mo.gov>
Sent: Wednesday, March 1, 2023 11:11 AM
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>; Winn, Jody <Jody.Winn@sos.mo.gov>
Subject: FW: Four sets of records involving FL and MO that need additional inspection.

See below

From: Totes Legit <toteslegitvotes@gmail.com>
Sent: Wednesday, March 1, 2023 10:40 AM
To: OECS@dos.myflorida.com; Elections-1 <Elections-1@sos.mo.gov>
Cc: Mercer, Kalen L. <Kalen.Mercer@dos.myflorida.com>; DivElections <DivElections@dos.myflorida.com>; SOSMain <sosmain@sos.mo.gov>
Subject: Four sets of records involving FL and MO that need additional inspection.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Hello Florida and Missouri!

Here are some sets of voter registrations between your two states who might belong to the same person per pair, and are listed by BOTH of your states as having voted in the 2020GE.

Please let me know you have received this email.

MO 73452070
FROST SARAH ELIZABETH
[redacted]
521 LINDA LN WENTZVILLE MO 63385
2020 General Election Voted
-- and --
FL LAK 103591740
FROST SARAH ELIZABETH
[redacted]
12910 SCOUT CT GRAND ISLAND 32735
NAS 103591740 11/03/2020 GEN E
-- detected by NCOA --
FROST SARAH ELIZABETH
521 LINDA LN WENTZVILLE MO 63385
12910 SCOUT CT GRAND ISLAND FL 32735-7801 LAKE
01/01/2021
-- other info --
[redacted]c7bcfa48-c234-4174-b4ac-559990c1f520?obtained_at=2021-11-17

AMERICAN OVERSIGHT

[redacted]a60ffcbf-3a4c-4758-ba87-6a0178bc26a3?obtained_at=2022-11-01
You might want to look at 2018GE, 2016GE, 2014GE, and others also.

MO 73538267
DECKER PAUL
[redacted]
23 HAVEN VIEW DR ST LOUIS MO 63141
2020 General Election Voted
-- and --
FL MAN 119334693
DECKER PAUL
15903 BAYCROSS DR BRADENTON 34202
[redacted]
MAN 119334693 11/03/2020 GEN E
-- detected by NCOA --
DECKER PAUL
23 HAVEN VIEW DR ST LOUIS MO 63141
15903 BAYCROSS DR LAKEWOOD RANCH FL 34202-2015 MANATEE
03/01/2021
-- other info --
[redacted]fdbfef47-8c3d-4f01-b271-e4156cb1f9bd?obtained_at=2021-11-17
[redacted]c58f12a9-d945-4762-b49e-cbe7d036a499?obtained_at=2022-11-01

MO 73134222
WING LINDA K
[redacted]
12801 MARYLAND ESTATES CT MARYLAND HEIGHTS MO 63043
2020 General Election Voted
-- and --
FL BRE 128384841
WING LINDA KAY
[redacted]
5055 DIXIE HWY NE APT B202 PALM BAY 32905
BRE 128384841 11/03/2020 GEN E
-- detected by NCOA --
WING LINDA K
12801 MARYLAND ESTATES CT MARYLAND HEIGHTS MO 63043
5055 DIXIE HWY NE APT B202 PALM BAY FL 32905-6611 BREVARD
10/01/2020
-- other info --
[redacted]fa2a06c-3546-4cb9-bb46-281ee889df75?obtained_at=2021-11-17
[redacted]4977011-ac3e-442a-b1d4-8b28f101d06f?obtained_at=2022-11-01

MO 73497152
JAMES KEITH BARKS
[redacted]
11421 BURGESS AVE BRIDGETON MO 63044
2020 General Election Voted
-- and --
FL OKA 125526871
BARKS JAMES KEITH
[redacted]
1699 HIGHWAY 98 W APT 403 MARY ESTHER 325691564
OKA 125526871 11/03/2020 GEN E
-- detected by NCOA --

AMERICAN OVERSIGHT

BARKS JAMES KEITH
1699 W HIGHWAY 98 APT 403 MARY ESTHER FL 32569-1564 OKALOOSA
11421 BURGESS AVE BRIDGETON MO 63044
12/01/2020
-- other info --
[redacted]bc410380-330e-4744-8f95-2dcd24a35abd?obtained_at=2021-11-17
[redacted] c859404-ad5c-4550-99d5-c9ce2e66e966?obtained_at=2022-11-01

==========

Totes Legit Votes
A citizen election integrity analyst

AMERICAN OVERSIGHT

From: Smartmatic newsletter <newsletter@smartmatic.com>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Date: 2/28/2023 2:33:52 PM
Subject: Newsletter: The Future of Election Technology

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

The Future is Here

Smartmatic's new line of innovative election technology can make voting more secure, faster and more transparent. Designed from the ground up to be compliant with new guidelines in the United States, the product line is available for election jurisdictions worldwide to begin previewing immediately.

READ MORE

5 Elements of Cybersecurity for Election Offices

This whitepaper will look at applied cybersecurity for elections. It will cite industry best practices and offer recommendations for self-guided organizational assessment and practical first steps toward better cybersecurity.

Read more

Belfer Center Election Cyber Incident Communications Plan Template

The Defending Digital Democracy Project has the goal to help secure elections against cybersecurity threats and information operations.

Read more

AMERICAN OVERSIGHT

IFES and Google partner on election security initiative

Pairing Google's expertise with IFES's long-held, trusted relationships with election officials, the partnership's goal is to bring the best in cybersecurity to elections.

Read more

Canada could become a leader in smart regulation of election technologies

Online voting has been used in Canada by numerous organizations, including political parties, unions and universities, as well as in local, provincial and territorial votes.

Read more

How Every Voting Experience Should Be

These are the 5 Cybersecurity Pillars to Protect an Election. Watch the video

CLICK HERE

Election Insight is powered by Smartmatic

Unsubscribe from this mailing list.

AMERICAN OVERSIGHT

From: John Rogers <john@redovoting.com>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
CC: Susan Craven Johnson <susan@bizcents.com>
Date: 2/26/2023 4:16:59 PM
Subject: EAC Election Security Grant - Missouri
Attachments: 8 POINTS.pdf
Template - FY23 State Request and Certification.pdf
Voluntary_Voting_System_Guidelines_Version_2_0.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Dear Director Peters,
Please find attached our recommended Election Security Grant submission for the state of Missouri, due to the Election Assistance Commission February 28, 2023, no later than 5:00 PM EST.

The Election Assistance Commission (EAC) is responsible for distributing, monitoring, and providing technical assistance to states and grantees on the use of funds allocated under the Help America Vote Act of2002 (HAVA). Grants for Election Security Funds were appropriated in 2018, 2020, 2022, and 2023 under Title I, Section 101 of HAVA. Missouri has applied for this grant each time it has been offered. According to the EAC, $16.5 million has been awarded to Missouri under this program, of which about 24% has been expended as of 9/30/2022.

Recognizing an opportunity to dramatically increase the integrity of voter rolls prior to elections and preserve that integrity throughout, Redo Voting has partnered with Bizcents, a data management company that cleans, parses, and structures election data. We have collaborated on producing a grant request to apply this clean data as voter roll management and input to the Redo Voting System, where it remains clean and protected throughout the election cycle with Redo Voting's exclusive access protocols.

These grants are submitted by the states for the effort, after which the state decides who will carry the effort based either on a competitive process between vendors or a sole source award based on exclusive capability. We are hoping for the latter, but that decision lies with the Secretary of State once the grant is approved and awarded.

We have provided herein the essential elements of our systems for your review. Our systems can provide your State with all necessary elements to safeguard your voter registration files, election files, and results. Our systems meet or exceed the current requirements articulated in the Voluntary Voter System Guidelines (VVSG 2.0).

We look forward to meeting with you soon to plan implementation.

Very Respectfully,
John

John G. Rogers DBA, Ph.D.
Founder & President
redovoting.com
john@redovoting
404.353.3052

AMERICAN OVERSIGHT

INTRODUCTION

The state of hereby requests grant monies to support the evaluation of innovative technologies to improve our election system. The state is specifically interested in a collaboration of two businesses offering unique, complementary technologies with promising potential to restore confidence and trust in our entire election system. Both businesses systems are fully developed and ready for deployment.

Bizcents LLC ["BCL"] developed a method to standardize state voter registration file data structure, update consistently all post-election data, identify potentially corrupt data requiring administrative action and flagging anomalies for further review. BCL is a woman-owned business.

Redo Voting LLC developed the Redo Voting System ["RVS"] which features open-source coding and highly sophisticated layered security measures in an easily accessible and usable package. Redo Voting LLC is a veteran-owned business.

The state intends to examine the licensing of BCL and the RVS to support the conduct of all future elections and associated voter file updates and management reviews for the reasons set forth below, among others:

- BCL offers an opportunity to ensure the reliability of the data contained in the state voter file by identifying anomalies requiring administrative action.
- BCL, once implemented, will reduce costs to administer the voter registration system and aid in the reduction of costs to run elections that the RVS will deliver.
- BCL provides the foundation for the RVS to operate at its peak efficiency.
- The RVS meets, exceeds or renders moot the fifteen principles enumerated by the federal EAC in its "Voluntary Voting System Guidelines 2.0".
- The RVS will reduce substantially the cost to administer elections while providing exceptional control over the election process, including recounts and challenges.
- The RVS is entirely transparent, which will restore our citizens' trust and confidence in elections conducted by this state. Its open-source coding stands in stark contrast to current voting machine suppliers who assert trade secret protection over their coding.

Following are more details about BCL and the RVS and the funding the state is requesting in the event the decision is made to deploy their systems prior to the 2024 election.

AMERICAN OVERSIGHT

1. VOTING EQUIPMENT

Budgeted Amount:
Percent of Budget:

The implementation of the RVS will require the purchase of new wholly dedicated servers, handheld scanners and other peripherals as outlined in attachment [X]. There are [x] total voting jurisdictions and [y] total precincts in the state which may need to be outfitted with [list equipment]. At this point we are assuming all precincts will need a full complement of new equipment.

The extent to which certain equipment already owned by the voting jurisdictions can be adapted to the RVS will be determined following a thorough inventory of such equipment. An adjustment to the budget will be made accordingly following the inventory, and a request for reallocation of excess funds or a return of excess funds will be made as circumstances warrant.

Acquired equipment will need security enhancements (i.e., ransomware protection, etc.) to comply with DOD, NIST and FISMA requirements. This requirement will apply also to existing equipment being adapted to the RVS.

Voting jurisdiction election officials will be trained and certified by the state to conduct elections using the RVS and new equipment. These officials will then be responsible for training at the local level.

The state confirms that all equipment and related purchases will be documented by paper purchase order, invoices or other instruments. Documentation will be scanned and digitized into the finance database for inspection via onsite or remote audit.

The state will also coordinate with its lottery department to identify equipment needs or, conversely, any equipment synergies that can be exploited with respect to ballot distribution and activation. Any needs will be quantified and added to the budget for later funding.

Existing voting equipment will be disposed in accordance with best practices. The state will coordinate the disposal process with the voting jurisdictions, including documentation of final disposition. Any costs incurred in connection with disposals will be documented as described in the preceding paragraph. Any funds received for scrap metal will be documented and used to offset costs in this budget area.

AMERICAN OVERSIGHT

2. VOTING PROCESSES

Budgeted Amount:
Percent of Budget:

Given the paradigm shift represented by the BCL / RVS combination, we believe that the state and its voting jurisdictions will achieve substantial cost reductions or eliminations in the defined activities which support the voting system. As such, we propose to do no spending in this area at this time.

3. VOTER REGISTRATION SYSTEMS

Budgeted Amount:
Percent of Budget:

The state is planning to review controls over the "Motor Voter" process in the context of the BCL / RVS operating environment now that the hiatus in implementing Real ID is lifted. The budgeted amount is primarily devoted to that control review.

The RVS does not directly impact the state's voter registration system. However, the state believes strongly that the implementation of the RVS will result in voters themselves taking the initiative to ensure their registrations are correct in all respects. The combination of voter initiative and behind-the-scenes BCL data management capabilities will serve to increase dramatically the reliability of the voter database over time.

See Voter Education (Section 6) below for additional information about encouraging all voters to validate their registrations, including events that would trigger a need to update one's voter registration.

4. ELECTION AUDITING

Budgeted Amount:
Percent of Budget:

Because the RVS operates online, there is a digital record of every administrative and voter transaction that occurs within the system. Privacy and voter anonymity are preserved because each voting transaction begins with a verified, but irreversible hashed voter registration accessing the voter's ballot slate. For each individual vote there is a digital signature proving that the vote went directly into the state's digital repository as submitted and remained there to be counted. The system can create printable pdfs of all ballots cast without ever revealing the identity of the voter.

AMERICAN OVERSIGHT

Fundamental reconciliations such as ballots issued to ballots cast can be completed with speed and accuracy. All ballots cast will be recorded in the appropriate jurisdictional voter file merely as the fact that an eligible, registered voter participated in the election. Basic reports like vote distribution tallies by candidate at the precinct level can be completed quickly and accurately without compromising voter anonymity.

Because of the inherent mathematical accuracy of the RVS, recounts can be conducted, if required, very quickly with no changes to the initial counts.

The state proposes to spend modest amounts to validate the benefits to the post-election audit process that are delivered by the RVS. The state believes that a well-maintained voter database using BCL will factor strongly into the success of post-election audits, as well as the acceptance of the results by candidates and voters alike.

Should other states adopt the BCL / RVS package, the ability to identify voters registered in more than one state would be greatly improved.

5. CYBER AND PHYSICAL SECURITY

Budgeted Amount:
Percent of Budget:

The RVS contains superior built-in controls which prevent unauthorized access to the voting system, including the state vote repository. Scratch-off QR codes, highly secure encryption features and electronic ballot activation are among the cybersecurity features which set the RVS apart from any other existing or proposed system. The combination of these controls with the lottery ticket printing and distribution controls used for ballot cards makes the RVS impregnable for all intents and purposes.

Additionally, inadvertent access or data manipulation is prevented, while all attempts to access the system are logged.

Since the RVS is an online application, legacy physical security requirements are greatly diminished. Personal physical security of the voter is enhanced by designing the vote casting process to occur anywhere, but only at times set by user protocols. As such, the amount budgeted will be used to identify and quantify the cost savings or eliminations that the state and its voting jurisdictions would realize.

6. VOTER EDUCATION

Budgeted Amount:
Percent of Budget:

AMERICAN OVERSIGHT

The RVS ensures that each legitimately registered voter could cast only one ballot, and that no one who is not a legitimately registered voter could cast a ballot at all. How this performance is made possible will be fully transparent to the public at any time as the RVS code is open-source. This unprecedented level of transparency will spark a restoration of voters' and candidates' faith and trust in every election. Not one of the competing system suppliers has ever made its coding available for public scrutiny. The uniqueness of the RVS and its confidence and trust restoring features will draw on-going attention from traditional media, which the state will leverage on its websites and social media assets.

The state will conduct voter awareness and education programs using a combination of its websites, social media assets, traditional media contacts, such as press releases, appearances on television and radio newscasts as well as participation in podcasts by interested third parties. The state will also reach out to state political party leaders to request they begin informing their members of the benefits of the RVS.

Local voter education projects will be supported through state-sponsored training and certification of election officers, basic printed materials for registrars' offices and downloadable materials from state and local voting jurisdiction websites.

The state will incorporate a feedback loop into its website to identify opportunities to improve messaging and voter understanding. The feedback loop will be called out in all media. It is possible that a third-party contractor would be engaged to manage the feedback and facilitate the gleaning of insights from the data collected.

Finally, the state will coordinate with the DMV about methods to communicate with holders of driver's licenses or state identification cards the need to update their voter registrations under certain conditions, such as moving into the state from another state or relocating within the state, including within the voting jurisdiction.

Regardless of whether a vote is cast in person or on-line, on election day, early or absentee, voters can be assured that their vote is cast privately and can never be traced back to them. Once a voter uses the ballot to cast his or her vote, that voter cannot cast another ballot until the next election.

The amount budgeted is primarily devoted to ensuring the public is completely informed about the RVS.

7. ACCESSIBILITY

Budgeted Amount:
Percent of Budget:

AMERICAN OVERSIGHT

The RVS ensures that every registered voter has unfettered access to the election process and the uncomplicated ability to legally exercise their right to vote.

Easily available ballots are immediately linked to a voter upon his or her receipt of it using available technologies. Driver's licenses or state identification cards are the most efficient means to link a voter to a ballot because all that's required is a scan of the identification code when the ballot is obtained. Only that voter can use that ballot to access the voter process and cast their fully anonymized vote.

Casting a ballot can be done privately on a camera-enabled, internet-capable device such as any smart phone (does not even have to be the voter's phone), a home desktop or laptop computer, a tablet, a public use computer at the library or even a work computer. Hence, a voter need not travel to a precinct on election day, or to an early voting location. Further, a voter need not worry about leaving the workplace. The state believes that the convenience offered by the RVS will serve to increase voter participation in future elections.

The budgeted amount primarily reflects the cost to design, print and distribute ballot cards to the public in advance of an election. There are no significant expenditures anticipated otherwise in this category.

8. OTHER

Budgeted Amount: N/A
Percent of Budget: N/A

On-going BCL data cleansing and standardization enable the state to avoid sharing raw data with interested parties. Regardless of whether states provide voter files to requesting parties for a fee or not, a better product will be made available.

Training of state election officials in the use of the BCL / RVS systems is included in the licensing fee.

AMERICAN OVERSIGHT

Template for State Requests for Security Funds

Mark Robbins, Interim Executive Director
U.S. Election Assistance Commission
633 3rd Street, NW, Suite 200
Washington, DC 20001

Dear Mr. Robbins:

The purpose of this letter is to request [$ amount] of the State of [Name]'s Help America Vote Act (HAVA) Election Security allocation.

The State of [Name] will use the funds provided under the HAVA Election Security grant program, for activities consistent with the laws described in Section 906 of HAVA and will not use the funds in a manner that is inconsistent with the requirements of Title III of HAVA.

We further certify that we have reviewed and accept the terms of the award as specified in the Fiscal Year 2023 Election Security Award Packet and Instructions. The signed terms and conditions, program narrative and combined budget have been uploaded to GrantSolutions as required.

Our UEI number (formerly DUNS) is [UEI number]. If you have any questions about this submission, please contact [Name] at [phone number] or [email].

Sincerely,

[Secretary of State Name]
[Title]

Cc.
Kinza Ghaznavi, Grants Director, HAVAFunding@eac.gov

AMERICAN OVERSIGHT

Voluntary Voting System Guidelines VVSG 2.0

Requirements for the Voluntary Voting System Guidelines 2.0

February 10, 2021

Prepared for the ***Election Assistance Commission***

At the direction of the
Technical Guidelines Development Committee

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000175

Acknowledgements

Chair of the TGDC:

Dr. Walter G. Copan
Director of the National Institute of Standards and Technology (NIST)
Gaithersburg, MD

Representing the EAC Standards Board:

Robert Giles
Director
New Jersey Division of Elections
Trenton, NJ

Paul Lux
Supervisor of Elections
Okaloosa County
Crestview, FL

Representing the EAC Board of Advisors:

Neal Kelley
Registrar of Voters
Orange County
Orange County, CA

Linda Lamone
Administrator of Elections
Maryland State Board of Elections
Annapolis, MD

Representing the Architectural and Transportation Barrier, and Compliance Board (Access Board):

Marc Guthrie
Public Board Member
Newark, OH

Sachin Pavithran
Public Board Member
Logan, UT

Representing the American National Standards Institute (ANSI):

Mary Saunders
Vice President, Government Relations & Public Policy
American National Standards Institute
Washington, DC

Representing the Institute of Electrical and Electronics Engineers:

Dan Wallach
Professor, Electrical & Engineering Computer Science
Rice University
Houston, TX

Representing the National Association of State Election Directors (NASED):

Lori Augino
Washington State Director of Elections
Washington Secretary of State
Olympia, WA

Judd Choate
State Elections Director
Colorado Secretary of State
Denver, CO

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000176

Individuals with technical and scientific expertise relating to voting systems and equipment:

McDermot Coutts
Chief Architect/Director of Technical Development
Unisyn Voting Solutions
Vista, CA

Geoff Hale
Computer Security Expert
Washington, DC

Diane Golden
Accessibility Expert
Grain Valley, MO

David Wagner
Professor, Electrical & Engineering
Computer Science
University of California-Berkeley
Berkeley, CA

AMERICAN OVERSIGHT

Public Working Groups discussed and developed guidance to inform the development of requirements for the VVSG.

- **The Election Process Working Groups: Pre-Election, Election, and Post-Election Process Working Groups** performed a great deal of up-front work to collect locale-specific election process information and, from that, to create coherent process models.
- **The Interoperability Working Group** handled voting system interoperability including common data format (CDF) modeling and schema development.
- **The Human Factors Working Group** handled human factors-related issues including accessibility and usability.
- **The Cybersecurity Working Group** handled voting system cybersecurity-related issues include various aspect of security control and auditing capabilities.
- **The Testing Working Group** handled voting system testing-related issues including what portions of the new VVSG need to be tested and how to test them.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000178

Executive Summary

The United States Congress passed the *Help America Vote Act of 2002 (HAVA) [HAVA02]* to modernize the administration of federal elections and to establish the U.S. Election Assistance Commission (EAC) to provide guidance to the states in their efforts to comply with the HAVA administrative requirements. *Section 202* of HAVA directs the EAC to adopt voluntary voting system guidelines, and to provide for the testing, certification, decertification, and recertification of voting system hardware and software.

The purpose of the guidelines is to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all the basic functionality, accessibility, and security capabilities required of voting systems. This document, the **Voluntary *Voting System Guidelines Version 2.0*** (referred to herein as the Guidelines or *VVSG 2.0*), is the fifth iteration of national level voting system standards. The Federal Election Commission published the first two sets of federal standards in 1990 *[VSS1990]* and 2002 *[VSS2000]*. The EAC then adopted Version 1.0 of the VVSG *(VVSG 1.0) [VVSG2005]* on December 13, 2005. In an effort to update and improve Version 1.0 of the VVSG, on March 31, 2015, the EAC commissioners unanimously approved *VVSG 1.1 [VVSG2015]*.

The *VVSG 2.0* is a departure from past versions in that a set of principles and associated guidelines were first developed to describe how, at a high-level, voting systems should be designed, developed, and how they should operate. The *VVSG 2.0* requirements were then derived from those principles and guidelines. The *VVSG 2.0* requirements fit within a framework of documents under the EAC Voting System Certification Program that include:

- VVSG 2.0 Principles and Guidelines
- VVSG 2.0 Requirements
- VVSG 2.0 Testing and Certification Program Manual

The Guidelines were designed to meet the challenges ahead, to replace decade's old voting machines, to improve the voter experience, and provide necessary safeguards to protect the integrity of the voting process. All sections of the prior VVSG versions have been reviewed, re-evaluated, and updated to meet modern expectations, which address how voters should interact with the voting system and how voting systems should be designed and developed. The *VVSG 2.0* requirements represent the latest in both industry and technology best practices, requiring significant updates in many aspects of voting systems.

The Guidelines allow for an improved and consistent voter experience, enabling all voters to vote privately and independently, ensuring votes are marked, verified and cast as intended, and that the final count represents the true will of the voters. *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]*, and *Web Content Accessibility Guidelines (WCAG) [W3C10]* are referenced and highlighted. Voter interface requirements have been updated to incorporate recent usability research and interactions that result from modern devices and now fully support accessibility throughout the voting process.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000179

The cybersecurity of voting systems has never been more important. Indeed, attacks from nation state actors on our elections infrastructure in 2016 led to a critical infrastructure designation. To limit the attack surface on voting systems, the Guidelines require that any election system, such as an e-pollbook or election reporting system, be air-gapped from the voting system. To ensure the integrity of the voting process, methods have been implemented to detect errors through the combined use of an evidence trail and regular audits, including risk-limiting audits (RLAs), compliance audits, and ballot-level audits. There is a dedicated section on ballot secrecy, preventing voter information from being carried through to the voting system, and two-factor authentication is now mandated for critical voting operations. Cryptographic protection of data and new system integrity requirements ensure that security protections developed by industry over the past decade are built into the voting system. These include risk assessment and supply chain risk management, secure configurations and system hardening, exploit mitigation, sandboxing and runtime integrity.

The *VVSG 2.0* requires the voting system to include the capability of using common data formats defined by the National Institute of Standards and Technology (NIST) and public working groups. The common data formats were created to make election data more transparent and interoperable. These formats can be used in addition to any native formats used by the manufacturer. Defensive coding practices, reliability and electrical requirements were reviewed, updated, and streamlined. Finally, guidance relevant to testing and certification has been moved to the EAC's testing and certification manual.

This document was produced by the EAC's Technical Guidelines Development Committee (TGDC) working in conjunction with NIST to aid in developing guidelines for voting equipment and technologies for making accessible, accurate and secure elections possible.

EAC staff must annually review the VVSG for proposed revisions. Determinations must be sent to the EAC's Executive Director (or a person operating in that capacity) to begin the review process required by HAVA (review by the TGDC, Board of Advisors, Standards Board, and public comment review) to ensure timely adoption of revisions. Under the direction of the Executive Director, EAC staff in consultation with NIST staff may make minor technical changes to the requirements in a timely manner. This process may include, but is not limited to, the development of an appeals process for such minor technical changes. EAC staff is responsible for updating the test assertions and issuing requests for interpretation or notices of clarification, as needed, to ensure efficiency in the process.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000180

Table of Contents

Acknowledgements 2
Executive Summary 5
Introduction 9
How the VVSG is to be Used 9
Scope 10
Implications for Networking and Remote Ballot Marking 12
External Network Connections 12
Remote Ballot Marking 13
Internal Wireless Networks 13
Major changes from VVSG 1.1 to VVSG 2.0 14
VVSG document structure 17
Conformance Information 17
Organization and Structure of VVSG 2.0 Requirements 17
Navigating through Requirements 18
Technical standards and terms used in the requirements 19
Conformance Language 19
Implementation Statement 20
Extensions to the VVSG 2.0 20
The VVSG 2.0 - Principles and Guidelines 21
Principle 1 High Quality Design 26
Principle 2 High Quality Implementation 64
Principle 3 Transparent 90
Principle 4 Interoperable 114
Principle 5 Equivalent and Consistent Voter Access 120
Principle 6 Voter Privacy 128
Principle 7 Marked, Verified, and Cast as Intended 133
Principle 8 Robust, Safe, Usable, and Accessible 168
Principle 9 Auditable 178
Principle 10 Ballot Secrecy 195
Principle 11 Access Control 204

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000181

Principle 12 Physical Security 219
Principle 13 Data Protection 226
Principle 14 System Integrity 235
Principle 15 Detection and Monitoring 250
Appendix A Glossary of Terms 262
Appendix B Requirements Listing 308
Appendix C References 321

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000182

Introduction

This document, the *Voluntary Voting System Guidelines 2.0* (*VVSG 2.0*), is the third version of national level voting system standards. Adherence to the Guidelines is governed by state and territory-specific laws and procedures.

VVSG 2.0 is a recommendation from the Technical Guidelines Development Committee (TGDC) to the Election Assistance Commission (EAC) for a voting system standard written to address the next generation of voting equipment.

This version offers a new approach to the organization of the guidelines. It is a complete re-write of the *Voluntary Voting System Guidelines 1.1 (VVSG 1.1) [VVSG2015]* and contains new and expanded material in many areas, including reliability, usability, accessibility, and security.

The requirements of the *VVSG 2.0* are more precise, more detailed, and written to be clearer to voting system manufacturers and test labs. The language throughout is written to be readable and usable by other audiences as well, including election officials, legislators, voting system procurement officials, various voting interest organizations and researchers, and the public at large.

The *VVSG 2.0* requirements were derived from the *VVSG 2.0 Principles and Guidelines*, which contain 15 major principles and 63 associated guidelines that cover voting system design, development, and operations.

How the VVSG is to be Used

This document will be used primarily by voting system manufacturers and voting system test laboratories as a baseline set of requirements for voting systems to which states will add their state-specific requirements as necessary. This audience includes:

- Manufacturers, who will use the requirements when they design and build new voting systems as information about how voting systems should perform or be used in certain types of elections and voting environments.
- Test labs who will refer to this document when they develop test plans for the analysis and testing of voting systems as part of the national certification process and state certification testing to verifying whether the voting systems have satisfied the *VVSG 2.0* requirements.

This document, therefore, serves as an important, foundational tool that defines a baseline set or requirements necessary for ensuring that the voting systems used in U.S. elections will be secure, reliable, and easy for all voters to use accurately.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000183

Scope

The scope of the *VVSG 2.0* is limited to equipment acquired by states and certified by the EAC. The *VVSG 2.0* covers pre-voting, voting, and post-voting operations consistent with the definition of a ***voting system*** in the *Help America Vote Act (HAVA) Section 301 [HAVA02]*, which defines a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; cast and count votes; report or display election results; and maintain and produce any audit trail information.

The ***voting system*** as defined in the *VVSG 2.0* is:

Equipment (including hardware, firmware, and software), materials, and documentation used to enact the following functions of an election:

1. *define elections and ballot styles,*
2. *configure voting equipment,*
3. *identify and validate voting equipment configurations,*
4. *perform logic and accuracy tests,*
5. *activate ballots for voters,*
6. *record votes cast by voters,*
7. *count votes,*
8. *label ballots needing special treatment,*
9. *generate reports,*
10. *export election data including election results,*
11. *archive election data, and*
12. *produce records in support of audits.*

As part of the voting system scope, *HAVA Section 301 [HAVA02]* mandates five additional functional requirements to assist voters. Although these requirements may be implemented in a different manner for different types of voting systems, all voting systems must provide these capabilities, which are reflected in the *VVSG 2.0* requirements:

1. Permit the voter to verify (in a private and independent manner) their choices before their ballot is cast and counted.
2. Provide the voter with the opportunity (in a private and independent manner) to change their choices or correct any error before their ballot is cast and counted.
3. Notify the voter if they have selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct their ballot before it is cast and counted.
4. Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for all voters.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000184

5. Provide alternative language accessibility pursuant to *Section 203* of the *Voting Rights Act [VRA65]*.

Section 301(a)(3)(B) [HAVA02] also states that there should be "… at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place". However, the *Americans with Disabilities Act of 1990 [ADA10]* requires that voters with disabilities be provided with auxiliary aids that allow them to participate equally in the voting process without discrimination. This is consistent with *Section 301* of HAVA cited above that requires a voting system to be accessible for individuals in a manner that provides the same opportunity for access and participation (including privacy and independence). If a majority of voters utilize hand-marked paper ballots, a sufficient number of accessible voting stations (including alternative language ballot features) must be available in each polling place to ensure their consistent availability in case of malfunctions. A sufficient number of machine-marked ballots must also be produced by those voting stations to ensure non-discrimination and ballot secrecy, particularly when the ballots produced by the accessible voting system differ in size, shape, and/or content from the hand-marked ballots and are thus readily identifiable. Procedures and training for poll workers on the operation of the accessible voting stations are also necessary to support this usage.

There is substantial experience[1] showing that having one accessible voting machine per polling place used only for voters with disabilities has worked poorly for voters with disabilities and may not be sufficient to provide equal access as required by law. For instance, data collected in recent elections highlight how difficult it is to ensure that a sufficient number of voters use the accessible voting machines to preserve the secrecy of machine-marked ballots and that poll workers are able to operate the machines successfully. To support best practices, states should consider legislation and additional resources to ensure balanced access to accessible voting machines wherever voting technology is deployed and used for elections.

The *VVSG 2.0* definition of a voting system does not expand the HAVA definition but focuses it on election processes. The *VVSG 2.0* principles, guidelines, and requirements apply to the election process functions and, by extension, to the voting devices that implement these functions.

The scope of most *VVSG 2.0* requirements apply to the entire voting system as opposed to specific devices, thus permitting the manufacturer more freedom to implement the requirements as they choose. However, when the scope of a requirement is limited to a specific function, that information is included in the text of the requirement, for clarity. For example:

- "A voting system's electronic display must be capable of..."

[1] For more details, see:
a) "Disability, Voter Turnout, and Voting Difficulties in the 2012 Elections" (Rutgers) **https://smlr.rutgers.edu/sites/default/files/images/Disability%20and%20voting%20survey%20report%20for%202012%20elections.pdf**;
b) "Experience of Voters with Disabilities in the 2012 Election Cycle" (National Council on Disability) **https://ncd.gov/rawmedia_repository/8%2028%20HAVA%20Formatted%20KJ%20V5%20508.pdf**; and
c) "The Blind Voter Experience: A Comparison of the 2008 and 2012 Elections" (National Federation of the Blind) **https://nfb.org/images/nfb/documents/word/2012_blind_voter_survey_report.docx**.

AMERICAN OVERSIGHT

- "Scanners and ballot marking devices must include…"
- "The cryptographic E2E protocol used in the voting system must…"

Implications for Networking and Remote Ballot Marking

Traditionally, ballots have been cast at polling places or through mail-in absentee ballots. There has been a growing trend to provide flexibility for voters to vote early and in-person at vote centers or at home using remote ballot marking applications. These innovative methods of voting provide additional paths to voting independently and privately for voters including those with disabilities. Likewise, advances in technology have led to efficiencies in election administration, including increasing the use of e-pollbooks for easy check-in and electronic election results reporting for timely aggregation of unofficial election results.

These additional election systems require network access to synchronize voter records, access remote ballot marking applications, and transmit unofficial election results. The measures taken to securing these systems falls outside the scope of *VVSG 2.0*. However, the benefits and risks associated with the use of these technologies was carefully considered when developing the Guidelines, whereas the associated and requirements were created developed to ensure that the voting system is isolated from these additional election systems.

This section clarifies the boundary between the external election systems and the voting system as well as the use of wireless technologies within polling places or vote centers.

External Network Connections

VVSG 2.0 does not permit devices or components using external network connections to be part of the voting system. There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., nation state attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected. These types of attacks include the following:

- The loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping.
- The loss of availability to access data or perform election process (e.g., ransomware attack).

The *VVSG 2.0* requirements address the concerns of external network connections (see *14.2-E – External network restrictions* and *15.4-B – Secure network configuration documentation)*. Externally networked devices or components, such as those used for e-pollbooks or transmission of election results, must be physically isolated from the voting system. This

AMERICAN OVERSIGHT

physical isolation can be described as an *air gap* between any systems that have an external network connection.

Remote Ballot Marking

Remote ballot marking is defined as an election system for voters to mark their ballots outside of a voting center or polling place. These systems are to be used as a tool which enables "no excuse" absentee voting. This allows a voter to receive a blank ballot to mark electronically, print, and then cast by returning the printed ballot to an election office. A voter may electronically fill out their ballot with a state-provided web application. Remote ballot marking applications provide another path to voting independently and privately for voters including those with disabilities.

The *VVSG 2.0* requirements apply to devices used to mark ballots inside a polling place or vote center. They do not apply to remote ballot marking devices and applications. The *VVSG 2.0* requirements affect only those voting system devices that constitute a voting system and that are submitted for testing and certification. For remote ballot marking, the voter uses a web application, their own personal device, and an external network (i.e., the Internet).

It should be noted that remote ballot marking applications need to comply with accessibility laws such as the *Americans with Disabilities Act of 1990 [ADA10]*. *VVSG 2.0* requirements that address the accessibility and usability for the electronic interface of a remote ballot marking software application can serve as an informative resource for developers of these systems. For example, *8.2-A — Federal standards for accessibility*, identifies the WCAG Level AA checkpoints in the *Section 508 [USAB18] – Standards* as a requirement for voting system electronic interfaces.

Internal Wireless Networks

Internal wireless networks wirelessly communicate or transfer information between two or more devices. Examples include use of wireless (Bluetooth) mice and keyboards or (Wi-Fi) printers. There are also growing trends towards using wireless technology for assistive devices such as headsets or hearing aids.

Wireless technology within the voting system introduces security concerns in that wireless networks can provide an entry point to the voting system for attackers. The security configurations for devices used in wireless technologies are not all equally secure, with some configured to provide more strength than others.

The *VVSG 2.0* requires that a voting system be incapable of broadcasting a wireless network (see *14.2-C – Wireless communication restrictions* and *15.4-C – Documentation for disabled*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000187

wireless). Instead, a voting system could use *wired* technology, e.g., Ethernet cables, to connect devices such as printers.

Wireless personal assistive technologies are still possible, however. A voter may use their Bluetooth headset by using an adapter connected to the voting system's 3.5 mm standard headphone jack, which creates a Bluetooth wireless connection between the adaptor and the headset. This effectively limits the attack surface to that of the headphone jack's analog communications without limiting the use of the voter's personal assistive technology.

Major changes from VVSG 1.1 to VVSG 2.0

There are many new or updated requirements, strengthening the security, interoperability, and usability and accessibility of voting systems.

Principle 1 - High Quality Design

- Functional equipment requirements are organized as phases of running an election:
    - Election and Ballot Definition
    - Pre-election Setup and logic and accuracy (L&A) testing
    - Opening Polls, Casting Ballots
    - Closing Polls, Results Reporting
    - Tabulation, Audit
    - Storage
- Requirements dovetail with cybersecurity in areas including:
    - Pre-election setup
    - Audits of barcodes versus readable content for ballot marking devices (BMDs)
    - Audits of scanned ballot images versus paper ballots
    - Audits of Cast Vote Record (CVR) creation
    - Content of various reports
    - Ability to match a ballot with its corresponding CVR
- Guidance relevant to testing and certification has been moved to the EAC testing and certification manuals.

Principle 2 - High Quality Implementation

- Adds requirement to document and report on user-centered design process by developer to ensure system is designed for a wide range of representative voters, including those with and without disabilities, and election workers

AMERICAN OVERSIGHT

Principle 3 – Transparent

- Addresses transparency from the point of view of documentation that is necessary and sufficient to understand and perform all operations

Principle 4 - Interoperable

- Ensures that devices are capable of importing and exporting data in common data formats
- Requires manufacturers to provide complete specification of how the format is implemented
- Requires that encoded data uses publicly available, no-cost method
- Uses common methods (for example, a USB) for all hardware interfaces
- Permits commercial-off-the-shelf (COTS) devices as long as relevant requirements are still satisfied

Principle 5 - Equivalent and Consistent Voter Access

- Applies to all modes of interaction and presentation throughout the voting session, fully supporting accessibility

Principle 6 - Voter Privacy

- Distinguishes voter privacy from ballot secrecy and ensures privacy for marking, verifying, and casting the ballot

Principle 7 - Marked, Verified, and Cast as Intended

- Updates voter interface requirements such as font, text size, audio, interaction control and navigation, scrolling, and ballot selections review
- Describes requirements that are voting system specific, but derived from federal accessibility law

Principle 8 - Robust, Safe, Usable, and Accessible

- References*, Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* and *Web Content Accessibility Guidelines 2.0 (WCAG 2.0) [W3C10]*
- Updates requirements for reporting developer usability testing with voters and election workers

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000189

Principle 9 - Auditable

- Focuses on machine support for post-election audits
- Makes software independence mandatory
- Supports paper-based and end-to-end (E2E) verifiable systems
- Supports all types of audits, including risk-limiting audits (RLAs), compliance audits, and ballot-level audits

Principle 10 - Ballot Secrecy

- Includes a dedicated ballot secrecy section
- Prevents association of a voter identity to ballot selections

Principle 11 - Access Control

- Prevents the ability to disable logging
- Bases access control on voting stage (pre-voting, activated, suspended, post-voting)
- Does not require role-based access control (RBAC)
- Requires multi-factor authentication for critical operations:
    - Software updates to the certified voting system
    - Aggregating and tabulating
    - Enabling network functions
    - Changing device states, including opening and closing the polls
    - Deleting the audit trail
    - Modifying authentication mechanisms

Principle 12 - Physical Security

- Requires using only those exposed physical ports that are essential to voting operations
- Ensures that physical ports are able to be logically disabled
- Requires that all new connections and disconnections be logged

Principle 13 - Data Protection

- Clarifies that there are no hardware security requirements (for example, TPM (trusted platform module))
- Requires Federal Information Processing Standard (FIPS) 140-2 *[NIST01]* validated cryptographic modules (except for end-to-end cryptographic functions)
- Requires cryptographic protection of various election artifacts
- Requires digitally signed cast vote records and ballot images
- Ensures transmitted data is encrypted with end-to-end authentication

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000190

Principle 14 - System Integrity

- Requires risk assessment and supply chain risk management strategy
- Removes non-essential services
- Secures configurations and system hardening
- Exploit mitigation (for example, address space layout randomization (ASLR) data execution prevention (DEP) and free of known vulnerabilities
- Requires cryptographic boot validation
- Requires authenticated updates
- Ensure sandboxing and runtime integrity

Principle 15 - Detection and Monitoring

- Ensures moderately updated list of log types
- Detection systems must be updateable
- Requires digital signatures or allowlisting for voting systems
- Requires malware detection focusing on backend PCs

VVSG document structure

This document contains the following sections:

- **Principles and Guidelines:** High level system design goals
- **Requirements:** Detailed technical requirements that support the principles and guidelines
- **Appendix A - Glossary of Terms:** Terminology used in requirements and informative language
- **Appendix B** - **List of all Requirements:** A summary listing of the titles of all requirements
- **Appendix C** - **References:** References to external sources used in the writing of the requirements

Conformance Information

This section provides information and requirements about how manufacturers can use the material in this document to assess whether a voting system conforms to the VVSG Principles and Guidelines. Conformance here means only that the requirements of the VVSG have been met; it does not imply certification according to the EAC's Voting System Certification Program.

Organization and Structure of VVSG 2.0 Requirements

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000191

The *VVSG 2.0* requirements are organized and numbered according to the principles and guidelines they are most applicable to. They have the following fields:

- Number and title of each requirement
- Text of each requirement
- Optional informative discussion field
- Optional informative field for applicability of the requirement

As an example, Requirement 8.1-B contains all four fields:

8.1-B – Flashing

If the voting system emits lights in flashes, there must be no more than three flashes in any one-second period.

Discussion

This requirement has been updated to meet *WCAG 2.0 [W3C10]* and *Section 508 [USAB18*] software design issue standards.

Applies to: Electronic interfaces

Requirements are indicated by the presence of a unique number in the left margin, followed by a descriptive title.

The Discussion field may aid in understanding the requirement but does not itself constitute a requirement.

The optional informative fields show related requirements and to which functions or devices of the voting system it applies:

- *"Related requirements:"* VVSG requirements elsewhere in the document related to the current requirement.
- *"Applies to:"* indicates the type of voting system function or device to which the requirement applies. This field is used only if the applicability of a requirement is not already clear in the requirement text.

Navigating through Requirements

You can navigate through the requirements:

AMERICAN OVERSIGHT

From the list of principles and guidelines in the *Table of Contents*. Links in this list navigate to the requirements that support each principle or guideline.

From the list of all requirements in *Appendix B: Requirements Listing*. This list lets you quickly identify requirements in each section. Each title is also linked to the requirement text for navigation throughout the document.

In addition, features of the Adobe Acrobat Reader can be useful. More information can be found in Adobe's help site under **Navigating PDF Pages**.

Technical standards and terms used in the requirements

There are a number of technical standards that are incorporated in the Guidelines through the use of references. These are referred to by title in the body of the document. The full citations for these publications are provided in *Appendix C: References*. This appendix also includes other references that may be useful for understanding the information. References in requirements and informative text are linked to *Appendix C*.

The requirements contain terms describing function, design, documentation, and testing attributes of voting system hardware, software, and telecommunications. Unless otherwise specified, the intended sense of technical terms is what is commonly used by the information technology industry. In some cases, terminology is specific to elections or voting systems. Requirements that use words with special meanings are linked to their definitions in *Appendix A: Glossary of Terms*.

Conformance Language

The text of a requirement is referred to as *normative*, meaning that the text constitutes the requirement and must be satisfied when implementing and testing the voting device or system. Text in this document that is not part of a requirement is referred to as *informative*, meaning that it is for informational purposes only and does not contain requirements.

The following keywords are used to convey conformance requirements:

"Must" indicates a mandatory requirement. Synonymous with "is required to."

"Must not" also indicates a mandatory requirement, but the requirement is to *not* do something.

"May" indicates an optional, permissible action and often suggests one possible way of conforming to a more general requirement.

What is neither required nor prohibited by the language of the requirements is permitted.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000193

Informative parts of this document include discussion, examples, extended explanations, and other matters that are necessary to understand the VVSG Principles and Guidelines and how to conform to them. Informative text may serve to clarify requirements, but it is not otherwise applicable to achieving conformance. Unless otherwise specified, a list of examples should not be interpreted as excluding other possibilities that were not listed.

Implementation Statement

A voting system conforms to the VVSG Principles and Guidelines if all stated requirements that apply to that voting system and all of its devices are fulfilled. The implementation statement documents the requirements that have been implemented by the voting system, the optional features and capabilities supported by the voting system, and any extensions (that is, additional functionality) that it implements.

The implementation statement may take the form of a checklist to be completed for each voting system submitted for conformity assessment. It is used by test labs to identify the conformity assessment activities that are applicable.

The implementation statement must include:

- Full product identification of the voting system, including version number or timestamp
- Separate identification of each device that is part of the voting system
- Device capacities and limits
- List of languages supported
- List of accessibility capabilities
- List of voting variations supported
- Devices that support the core functions and how they do it
- List of requirements implemented
- Any extensions also included in the voting system
- Signed document that the information provided accurately characterizes the system submitted for testing

Extensions to the VVSG 2.0

Extensions are additional functions, features, or capabilities included in a voting system that are not defined in the requirements. Extensions are permitted to accommodate the needs of states that may impose additional requirements and to accommodate changes in technology. However, an extension is not allowed to contradict or relax requirements that would otherwise apply to the system and its devices.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000194

The VVSG 2.0 - Principles and Guidelines

The *VVSG 2.0* consists of 15 principles and 53 guidelines. Together these principles and guidelines cover voting system design, development, and operations.

Principle 1: HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly accepted election process specifications.

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

Principle 2: HIGH QUALITY IMPLEMENTATION

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

2.2 - The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

2.5 - The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in anticipated physical environments.

Principle 3: TRANSPARENT

The voting system and voting processes are designed to provide transparency.

AMERICAN OVERSIGHT

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

Principle 4: INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

Principle 5: EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

Principle 6: VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others.

AMERICAN OVERSIGHT

Principle 7: MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities.

8.4 - The voting system is evaluated for usability with election workers.

Principle 9: AUDITABLE

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

Principle 10: BALLOT SECRECY

The voting system protects the secrecy of voters' ballot selections.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000197

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

Principle 11: ACCESS CONTROL

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

Principle 12: PHYSICAL SECURITY

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

Principle 13: DATA PROTECTION

The voting system protects data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000198

Principle 14: SYSTEM INTEGRITY

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.2 - The voting system is designed to limit its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Voting system software updates are authorized by an administrator prior to installation.

Principle 15: DETECTION AND MONITORING

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system is designed to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000199

Principle 1
High Quality Design

HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 - The voting system is designed using commonly accepted election process specifications.

1.2 - The voting system is designed to function correctly under real-world operating conditions.

1.3 - Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000200

Principle 1
HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

The requirements for *Principle 1* and its guidelines include functional requirements for election definition and preparation through all voting processes concluding with closing of the polls, tabulating, and reporting. The requirements deal with how voting systems are designed to operate during election processes, including limits for stress and volume. Other principles provide more detailed requirements in other areas including accessibility, security, and usability.

The requirements for ***Guideline 1.1*** are arranged into sections by election process with requirements containing the basic core requirements for conducting an election:

1 – Election definition which deals with the capabilities of the voting system to define an election, that is, manage items such as election districts, contests, candidates, and to define ballots for the election that may be specific to various combinations or splits of precincts. Support for the specifications described in the Election Results Common Data Format Specification *(NIST SP 1500-100) [NIST16]* is required for imports and exports.

2 – Pre-election testing which deals with capabilities of the voting system to configure and verify correctness of devices before opening the polls. Logic and accuracy (L&A) testing is covered here, as well as new requirements to check that cast vote records (CVR) are created properly and that any encoded data such as barcodes is accurately recorded.

3 - Opening the polls which deals with capabilities of the voting system to ensure that the voting system is properly configured so that polls can be opened.

4 - Casting which deals with the capabilities of the voting system to enable a voter to activate and cast a ballot. If ballot activation occurs on an electronic pollbook, one cannot test and verify whether these requirements are satisfied unless the entire pollbook is also tested. Additionally, the requirements deal with capabilities needed for common vote variations, ballot measures, and write-ins.

5 - Recording voter choices which deals with casting ballots and how equipment will handle ballots as they are cast, including the processes involved in recording votes in cast vote records. This mandates recording the selected contest options, and other information needed for linking the CVR with the device that is creating the CVRs and for auditing.

AMERICAN OVERSIGHT

6 – Ballot handling for vote-capture devices which deals with functions that scanners will provide, including separating ballots for various reasons, for example, because of write-ins on manually-marked paper ballots and handling mis-fed ballots. It deals with the behavior of batch-fed scanners and voter-facing scanners when scanning ballots that need manual handling or inspection, such as for write-ins or unreadable ballots.

7 – Exiting or suspending voting which deals with exiting the voting mode (closing the polls), that is, stopping voting and preventing further voting. This applies to those systems located at a remote location such as the polling place or vote centers.

8 – Tabulation which deals with how tabulation processes will handle voting variations, including those methods used most commonly across the United States.

9 - Reporting results which deals with the need for the voting system to have the capability of creating all required precinct post-election reports. This includes recording ballots such as absentee ballots and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots.

The requirements for ***Guideline 1.2*** cover how a voting system is designed to function correctly under real-world operating conditions. They address:

- **Reliability** – the failure rate benchmark for reliability, the need to protect against a single point of failure, and the need for systems to withstand the failure of input and storage devices.
- **Accuracy** – the need to satisfy integrity constraints for accuracy, to achieve the required end-to-end accuracy benchmark, and the ability to reliably detect marks on the ballot.
- **Misfeed rate** – which treats all misfeeds, such as multiple feeds, jams, and ballot rejections collectively as "misfeeds" and the need to meet the misfeed rate benchmark.
- **Stress** – the ability to respond gracefully to all stresses of the system's limits.
- **Election volume** –the ability to handle a realistic volume of activities in normal use throughout an entire election process.

The requirements for ***Guideline 1.3*** cover how voting system design supports evaluation methods that enable testers to distinguish a system that correctly implements specified properties from those that do not. They include:

- **Reporting of manufacturer-performed tests** – so testers have a baseline set of information significant for the specification, performance, and reporting of each test.
- **Coverage of manufacturer-performed tests**– so that all requirements applicable to a submitted system are also covered by submitted tests.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000202

1.1 – The voting system is designed using commonly-accepted election process specifications.

1.1.1 – Election definition

1.1.1-A – Election definition

The voting system must provide the capability to import, define, maintain, and export the information necessary to define ballots and hold an election, including for:

1. election districts,
2. contests and ballot measures,
3. candidates, and
4. ballot style information.

Discussion

This requirement states that election and ballot definition capabilities must be included within the voting system. Ballot style information includes those labels, headers, and other information typically found on ballots and that varies across jurisdictions and precincts. Requirements in *Principle 4: Interoperable* deal with using common data formats for importing and exporting election definition information.

1.1.1-B – Serve multiple or split precincts and election districts

The voting system must describe election districts and precincts in such a way that a given polling place may serve:

1. two or more election districts; and/or
2. combinations of precincts and split precincts.

Discussion

This requirement addresses the capability to accommodate multiple ballot styles depending on the political geography being served by a polling place.

1.1.1-C – Multiple identifiers

The voting system must enable election officials to associate at least three identifiers that can be cross-referenced with each other for administrative subdivisions, election districts, contests, and candidates. This also includes:

AMERICAN OVERSIGHT

1. locally defined identifiers;
2. state-wide-defined identifiers; and
3. Open Civic Data Identifiers [OCD-ID].

Discussion

This requirement is based on the need to support cross-referencing of statewide identifier schemes, such as *Open Civic Data Identifiers [OCD-ID]* with those used on a more local level.

1.1.1-D – Definition of parties and contests

The voting system must allow for:

1. the definition of political parties and indicate the affiliation or endorsements of each contest option;
2. information on both party-specific and non-party-specific contests, with the capability to include both contests on the same ballot; and
3. contests that include ballot positions with write-in opportunities.

1.1.1-E – Voting variations

The voting system must provide the capability to define and identify contests, contest options, candidates, and ballot questions using all voting variations indicated in the manufacturer-provided implementation statement.

Discussion

See requirements in sections *1.1.4 – Casting* and *1.1.8 – Tabulation* for voting variations most commonly used in the U.S.

1.1.1-F – Confirm recording of election definition

The voting system must check and confirm that its data is correctly recorded to a persistent storage system.

Discussion

Persistent storage includes storage systems such as non-volatile memory, hard disks, and optical disks.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000204

1.1.1-G – Election definition distribution

The voting system must provide for creation of master copies of election definition information as needed to configure each voting device in the voting system.

1.1.1-H – Jurisdiction-dependent content

The voting system must enable election officials to update jurisdiction-dependent text, line art, logos, and images to ballot styles.

1.1.1-I – Include contests

The voting system must provide for the inclusion of all contests in a given ballot style, in which the voter is entitled to vote.

1.1.1-J – Exclude contests

The voting system must provide for the exclusion of any contest from a given ballot style, in which the voter is prohibited from voting because of place of residence or other administrative criteria.

Discussion

In systems supporting primary elections, this requirement would include the exclusion of party-specific contests for which voters in a particular political party are not eligible to vote.

1.1.1-K – Primary elections, associate contests with parties

The voting system must support the association of different contests with different political parties when administering primary elections.

1.1.1-L – Ballot rotation, Election definition

The voting system must support the production of rotated ballots or activating ballot rotation functions in vote-capture devices by including relevant metadata in distributed election definitions and ballot styles.

1.1.1-M – Ballot configuration in combined or split precincts

The voting system must include the capability of creating distinct ballot configurations for voters from two or more election districts that are served by a given polling place or vote center.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000205

1.1.1-N – Ballot style identification

The voting system must include the capability to generate codes or marks to uniquely identify the ballot style associated with any ballot.

1.1.2 – Pre-election testing

1.1.2-A – Built-in self-test and diagnostics

The voting system must include built-in measurement, self-testing, and diagnostic software and hardware for monitoring and reporting the system's status.

1.1.2-B – Installation of software and ballot styles

The system must include the capability to verify that software and ballot styles have been properly selected and to provide notification of any errors that occur while selecting or installing software and ballot styles.

Discussion

At a minimum, *notification* means an error message and a log entry. Examples of detectable errors include use of software or data intended for a different type of device or operational failures in transferring the software or data.

1.1.2-C – Use of test ballots

The voting system must provide the capability to submit test ballots for use in verifying the integrity of the system.

1.1.2-D – Testing all ballot positions

Vote-capture devices must allow for testing that uses all potential ballot positions in the election as active positions.

1.1.2-E – Testing cast vote record creation

The voting system must include the ability to verify that cast vote records (CVRs) are created and tabulated correctly by permitting election officials to compare the created CVRs with the test ballots.

Discussion

This requires providing a capability such as an export of CVRs and a tabulated summary that can be compared manually against their test ballot counterparts.

AMERICAN OVERSIGHT

1.1.2-F – Testing codes and image creation

The voting system must include the capability to verify that encoded versions or images of voter selections on a ballot and any other encoded information on a ballot are created correctly by permitting election officials to compare the encodings and images with the test ballots.

Discussion

The purpose of this requirement is to give election officials the capability, prior to opening the polls, to audit encoded versions of voter selections. This process may include the review of created ballots and encoded information on each ballot to ensure that the images correctly match the ballot, thus validating accuracy in ballot creation. and that the ballot was created accurately. will include such as provided by a ballot marking device (BMD) using QR codes and gain assurance that the QR codes and any encoded data represented by the QR codes contains the voter's selections exactly as made. Likewise, to audit any image of the ballot made by a scanner to gain assurance that the image correctly matches the ballot. And, to audit any encoded information on the ballot to gain assurance it is being created correctly.

Related requirement: 1.1.2-C – Use of test ballots

1.1.2-G – Testing equipment calibration

Scanners must support testing the calibration of the paper-to-digital conversion (such as the calibration of optical sensors, the density threshold, and the logical reduction of scanned images to binary values, as applicable).

1.1.2-H – No side-effects from pre-election testing

Pre-election testing must introduce no lasting effects in regard to the operation of the voting system during the election other than:

1. audit log entries;
2. status changes to note that the tests have been run with a successful or failed result;
3. separate storage of test results;
4. changes in counters that record ballots cast; and
5. normal wear and tear.

Discussion

It should be impossible (by design) for the pre-election testing to have any influence on the operation of the device(s) during the election or on the results that are reported for the election. Most notably, election results can never include any test votes that were counted during pre-election testing. If a test election is run on the voting system as a means of providing pre-election testing, an election

AMERICAN OVERSIGHT

official should be able to remove all artifacts of the test election except as noted in items 1 through 5 of this requirement.

1.1.2-I – Equipment status and readiness reports

The voting system must provide the capability to produce equipment readiness reports that show the readiness of the equipment, including:

1. whether calibration is needed;
2. consumable supplies such as toner or paper are sufficient for use;
3. batteries are fully charged; and
4. the status of other election-sensitive aspects of the equipment.

1.1.2-J – Ballot style readiness reports

The voting system must provide the capability to produce pre-election reports that include:

1. the allowable number of votes in each contest;
2. the tabulation method for each contest;
3. the inclusion or exclusion of contests as the result of precinct splits; and
4. samples of all final ballot styles.

1.1.2-K – Precinct-based voting devices readiness reports

Precinct-based voting devices must have the capability of generating readiness reports that include:

1. the election's identification data;
2. the identification of the precinct and polling place; and
3. the identification of all ballot styles used in that precinct.

1.1.2-L – All vote-capture devices readiness reports

Vote-capture devices must have to capability to generate a report that includes the following:

1. the election's identification data;
2. the identification of the precinct and polling place, if applicable;

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000208

3. the identification of the device;
4. the identification of all ballot styles loaded;
5. the contents of each active contest option register at all storage locations;
6. confirmation that no hardware or software failures were detected during setup and testing, or a record of those that occurred; and
7. any other information needed to confirm the readiness of the equipment.

1.1.3 – Opening the polls

1.1.3-A – Opening the polls

The voting system must provide functions to enter a mode in which voting is permitted.

Discussion

This and following requirements cover the process of enabling voting to occur by placing the voting system in a voting mode. More information about the activated stage is defined in Table 11-1.

1.1.3-B – Non-zero totals

The voting system must not enter the voting mode until all steps necessary to isolate test data from election data have been performed successfully and all vote counters have been zeroed. An attempt to open polls with non-zero counters:

1. must be recorded in the audit log, and
2. an election worker must be clearly notified of the event.

Discussion

Jurisdictions that allow early voting before the traditional election day should document that a distinction is made between the opening and closing of the polls. This can occur only once per election, and the suspension and continuance of voting between days of early voting. The open-polls operation, which requires zeroed counters, is performed only when early voting commences; the continuation of voting that was suspended overnight does not require that counters be zeroed again.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000209

1.1.4 - Casting

This section describes the requirements of the ballot issued to the voter and the types of contests that appear on the ballot. This includes characteristics that the voter must be aware of in order to accurately reflect the intent of their choices and the requirements of the voting system when the ballot is cast.

1.1.4-A – Voting and casting the ballot

The voting system must provide a ballot to each voter containing contests and contest choices using all voting variations that are indicated in the voting system implementation statement.

1.1.4-B – Control ballot configuration

The voting system must, where applicable:

1. activate all portions of the ballot the voter is entitled to vote on;
2. disable all portions of the ballot the voter is not entitled to vote on; and
3. enable the selection of the ballot configuration that is appropriate to the party affiliation declared by the voter in a primary election.

Discussion

This requirement does not apply to pre-printed paper ballots. For on-demand ballot printing systems, item 3 requires that the proper ballot style be selected for the voter and the appropriate ballot be printed for the voter's use. For an electronic display or ballot marking device, items 1-3 would be required, where poll workers may control the ballot configuration by using an activation device, issuing a token, or following other jurisdictional procedures to select the appropriate ballot style.

1.1.4-C – Precinct splits, Casting

Each ballot that is issued to a voter must include contests that are associated with a district that the voter's residential address falls within.

Discussion

If a precinct is not entirely contained in the district associated with the precinct, multiple ballot styles must be available to ensure that each voter in the precinct receives a ballot that only contains contests for which they are eligible to vote.

AMERICAN OVERSIGHT

1.1.4-D – Ballot rotation, Casting

The order of contest options listed on each ballot must be in the order prescribed. The voting system must be able to correctly associate a voter's choice with the associated contest choice independent of where it appears on a specific voter's ballot.

Discussion

Many states require contest choice position order to be rotated on different ballots to prevent bias for or against a choice based on position listed.

1.1.4-E – Partisan closed primary ballot

The voting system must provide a type of ballot, used in a partisan primary election. to the voter that only contains contests associated with a specific party to which the voter is registered in addition to any nonpartisan contests that the voter is eligible to make choices.

Discussion

This type of ballot is used in states that run *closed primary elections* (voter is issued a ballot based on party of registration), *partially closed primary elections* (voter can receive a party-specific ballot that is different from their registration or an unaffiliated voter can choose a party ballot) and *partially open primary elections* (voters do not register by party and choose a party-specific ballot for the election).

1.1.4-F – Partisan open primary ballot

The voting system must provide a type of ballot, used in a partisan primary election, to the voter that contains partisan contests from all parties and any nonpartisan contests in which the voter is eligible to make choices. Only choices associated with one party will be permitted.

Discussion

This type of ballot is used in states that run *open primary elections*, where voters do not register by party but choose the party for which they wish to vote.

1.1.4-G – Indicate party affiliations and endorsements

The voting system must provide a type of ballot associated with:

1. a *partisan primary election* that identifies the party associated with each listed primary election contest (all listed contest options are affiliated with the listed party); and

AMERICAN OVERSIGHT

2. a *partisan general election* that identifies the affiliated/endorsing party of each contest choice.

1.1.4-H – Write-in contest options

The voting system must be capable of enabling and recording the voter's write-in of desired candidate names.

Discussion

A write-in is a contest option on the ballot that permits the voter to identify a candidate of choice that is not already listed as a contest option and is captured when the ballot is cast. State rules determine when a write-in candidate option may be placed as a contest option on the ballot and what qualifies as a valid write-in selection that may be counted.

1.1.4-I – Write-in reconciliation

The voting system must be capable of gathering and recording write-in votes within a voting process that allows for reconciliation of aliases and double votes.

Discussion

Reconciliation of aliases means allowing election officials to declare two different spellings of a candidate's name to be equivalent (or not). Reconciliation of double votes means handling the case where, in an N-of-M contest, a voter has attempted to cast multiple votes for the same candidate using the write-in mechanism.

1.1.4-J – N-of-M contest, Casting

For the N-of-M contest, the voting system must be capable of gathering and recording votes in a contest where the voter may choose up to a specified number of choices from a list of contest options. These selections are independent of selections in any other contest.

Discussion

A baseline N-of-M contest is one where a voter is allowed N contest choices from a list of M choices and where votes are tallied independently of any other contest options on the ballot. N includes 1 (vote for 1 contest or typically a measure) or any larger number. If N is larger than M, all choices listed will be selected. It can be used for *approval voting* by setting N equal to M. It can also be used for *limited voting* by setting N to be less than the number of seats being elected.

1.1.4-K – Straight-party voting, Casting

For straight-party voting, the voting system must be able to provide a contest in which a voter may select political party contest choices that result in the selection of all partisan

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000212

contests on their ballot. In this instance, a selection of a political party choice automatically selects all contest choices associated with that party. The voting system must be capable of gathering and recording votes for both this contest and all partisan contests associated with it.

Discussion

Straight-party voting is a voting variation used in a general election. It provides the voter with the ability to select all candidates affiliated with a desired party in all partisan contests on the ballot by selecting one contest option. When a party is selected, the system must not prevent the selection of individual candidate options that may negate the original straight-party choice, nor must it require that voters utilize the straight-party voting option. Rules for determining the candidate choices resulting from the combination of direct option selections and straight-party option selections are determined by the rules in states that use straight-party voting.

1.1.4-L – Cumulative voting contest, Casting

For a cumulative voting contest, the voting system must be capable of gathering and recording votes in a contest where the voter may allocate no more than the allowed number of votes to one or more contest selections in whole vote increments.

Discussion

When a cumulative voting contest is on a ballot, the system must allow the voter to assign all allowed votes to any desired contest selection or to any set of contest selections in whole vote increments. The total of all selection assignments must not exceed the total votes allowed. (See *1.1.4-Q - Proportional voting contest (equal-and-even cumulative voting contest), Casting* for an alternate method of assigning multiple votes to a candidate.)

1.1.4-M – Ranked choice voting contest, Casting

For a ranked choice voting (RCV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest selections in order of preference, as first choice, second choice, etc.

Discussion

The ballot presentation of a RCV contest is independent of the number of seats being elected. Depending on jurisdictional rules, the number of choice options provided may vary from a minimum of 3 to the number of contest choices on the ballot. Contest outcome determination requires cast vote records (CVR) to be processed post-election.

AMERICAN OVERSIGHT

1.1.4-N – Party preference contest

For a party preference contest, the voting system must be capable of gathering and recording votes for a contest containing a list of political party choices. In this instance, the voting system uses a valid selection of a party in the contest, which limits gathering and recording of votes in all partisan contests on the ballot to those associated with the selected party.

Discussion

A party preference contest only appears on an *open primary ballot* when required by state rules. Its purpose is to allow the voter to select the party they intend to vote contests for and prevent the voter from spoiling the partisan section of the ballot by, for example, marking contests in a different party's section of the ballot.

1.1.4-O – Top-2 primary contest (blanket primary contest)

For a top-2 primary contest, the voting system must be capable of assigning candidates of all relevant parties to a single seat contest which is also assigned to all partisan ballots.

Discussion

In some states, this method is required to be used to fill designated partisan offices. The contest, also called a *blanket primary contest*, appears on all party-specific primary ballots. All candidates are listed as contest options including their party affiliation. The 2 candidates who receive the most votes will be on the general election ballot independent of their party affiliation.

1.1.4-P – Presidential delegate contest, Casting

For a presidential delegate contest, the voting system must be capable of gathering and recording votes for only those delegates that are affiliated with the voter's choice in the presidential preference contest.

Discussion

Presidential delegate voting is a voting variation that only is used in a *presidential primary election* on a party-specific primary ballot where delegates to the convention are selected by the voter when the method is selected by a state's political party. With this method, only contest option selections in delegate contests that are pledged to the voter's presidential candidate selection will be recorded. If the voter does not make a selection in the presidential preference contest, selections for presidential delegates will not be recorded.

AMERICAN OVERSIGHT

1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting

For a proportional voting contest, the voting system must be capable of gathering and recording votes for a contest which allow multiple votes to be assigned to a candidate. This is accomplished by prorating the number of allowed votes proportionally to the number of validly selected candidates.

Discussion

Also known as *equal-and-even cumulative voting*, this contest is an alternative to a cumulative voting contest in allowing multiple votes to be assigned to selected candidates. Votes are assigned based on the votes allowed and the number of valid selections made by dividing the number of votes allowed by the number of options chosen. Marking fewer selections than the number of votes allowed may result in fractional votes being assigned to a contest option.

1.1.4-R – Group voting contest, Casting

For a group voting contest, the voting system must be capable of designating a group select contest choice that automatically selects, gathers and records all contest choices associated with the group. More than one contest group select contest choice must be provided if the contest contains more than one group of candidates.

Discussion

A group voting contest is used to enable the voter to select a large number of allowed candidate options associated with a single group, party or ideology with a single option selection. There may be multiple groups of contest choices each associated with a single selection. The system treats a group selection as if all candidates in the group are selected when determining the number of selections made. This voting variation is currently only used in the State of Massachusetts to select Ward and Town party committee persons and only appears on the ballot in the presidential preference primary.

1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)

For a top-2 instant runoff voting (IRV) contest, the voting system must be capable of gathering and recording votes in a contest where the voter must be able to rank contest options in order of preference as their first choice, second choice, etc.

Discussion

The top-2 IRV contest, also known as a supplementary or contingent vote contest, is an IRV type contest and provides the voter the ability to identify the contest options in order of preference in the same fashion as a standard IRV contest. Although voted the same as an IRV contest and requiring cast vote records to be processed post-election to determine outcome, only the top-2 candidates with the most votes are eligible to win.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000215

1.1.5 – Recording voter choices

1.1.5-A – Casting and recording

The voting system must support casting a ballot, recording each vote precisely as indicated by the voter subject to the rules of the election jurisdiction, and creating a cast vote record that can be tabulated and audited.

1.1.5-B – Ballot orientation

The voting system, when using pre-printed ballots, must either:

1. correctly mark pre-printed ballots regardless whether they are loaded upside down, right side up, forward, or reversed; or
2. detect and reject pre-printed ballots that are oriented incorrectly.

1.1.5-C – Record contest selection information

The voting system must record contest selection information in the CVR that includes:

1. all contest selections made by the voter for all supported vote variations; and
2. positions on the ballot associated with each contest selection made by the voter when multiple selections are permitted, if applicable.

Discussion

For item 2, some contests such as for RCV may place candidate choices on the same line of the ballot, therefore the positions of the candidates may need to be recorded.

1.1.5-D – Record write-in information

The voting system must record write-in information in the CVR that includes:

1. identification of write-in selections made by the voter;
2. the text of the write-in, when using a BMD or other device that marks the ballot for the voter;
3. an image or other indication of the voter's write-in markings; and
4. the total number of write-ins in the CVR.

AMERICAN OVERSIGHT

1.1.5-E – Record election and contest information

The voting system must record additional contest information in the CVR that includes:

1. identification of all contests in which a voter has made a contest selection;
2. identification of all overvoted and undervoted contests;
3. the number of write-ins recorded for the contest; and
4. identification of the party for partisan ballots or partisan contests.

Discussion

For identification of the party, a ballot in a *partisan primary election* may in some cases contain contests for different parties. Thus, an indication as to partisanship of the contests is required.

1.1.5-F – Record ballot selection override information

The voting system, if recording voter selections differently than as marked due to election or contest rules in effect, must record information in the CVR that includes:

1. identification of the original ballot selections made by the voter;
2. identification of the changed voter selections; and
3. identification of the reasons for the changes.

Discussion

When marking a ballot by hand, a voter may vote in contests in which the voter is not allowed to make contest selections. For example, a voter may elect to vote straight-party, but then make contest selections in contests which differ from the political party contest choices. Election or contest rules may cause a scanner to invalidate the contest markings or require other actions.

1.1.5-G – Record audit information

The voting system must be capable of recording audit-related information in the CVR or collection of CVRs as they are created, that includes:

1. identification of the specific creating device such as a serial number;
2. identification of the geographical location of the device;
3. identification of the ballot style corresponding to the CVR;
4. identification of the corresponding voted ballot;
5. for multi-sheet ballots, identification of the individual sheet corresponding to the CVR, along with the identification of the ballot style;

AMERICAN OVERSIGHT

6. identification of the batch containing the corresponding voted ballot, when applicable; and
7. sequence of the corresponding voted ballot in the batch, when applicable.

Discussion

Item 2 can be any identification scheme that is preferential in the jurisdiction, e.g., polling place name, address, geographical coordinates, etc.

Item 4 can be satisfied by printing a unique ID on the ballot as it is scanned and including that ID in the corresponding CVR.

Item 5 ensures that every sheet of a multi-sheet ballot contains the sheet number as well as the ballot style ID. This way, a ballot style ID could be defined to include all sheets, or each sheet could be defined with a unique ballot style.

Items 6 and 7 are necessary when ballot batching is in effect.

1.1.5-H – Store and link corresponding image

The voting system must be capable of storing an image of a paper ballot and linking this image to the specific associated CVR.

Discussion

The image could be linked to the CVR by, for example, creating a filename for the image that is the same as the identifier from item 4 in Requirement *1.1.5-G – Record audit information*.

1.1.6 – Ballot handling for vote-capture devices

1.1.6-A – Detect and prevent ballot style mismatches

The voting system must detect ballot style mismatches and prevent votes from being tabulated or reported incorrectly due to a mismatch.

Discussion

For example, if the ballot styles loaded on a scanner disagree with the ballot styles that were used by vote-capture devices, the system will raise an alarm and prevent the incorrect ballot styles from being used during tabulation. Otherwise, votes could be credited to the wrong contest options.

Such a mismatch should have been detected and prevented during L&A testing but if it was not, it needs to be detected and prevented before tabulation begins.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000218

1.1.6-B – Detect and reject ballots that are oriented incorrectly

The voting system must either:

1. correctly count ballots regardless of whether they are fed upside down, right side up, forward, or reversed; or
2. detect and reject ballots that are oriented incorrectly.

1.1.6-C – Ballot separation when batch feeding

Batch-fed scanners, in response to unreadable ballots, write-ins, and other designated conditions, must do one of the following:

1. out stack the ballot (that is, divert to a stack separate from the ballots that were normally processed);
2. stop the ballot reader and display a message prompting the election official to remove the ballot;
3. mark the ballot with an identifying mark to facilitate its later identification; and/or
4. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot.

Discussion

Item 4 allows the ballot image to be segregated if, for example, an identifier is printed on the ballot as it is scanned, so that the image of the ballot also contains this identifier. Without a unique identifier or other marking, the ballot image itself does not facilitate finding the corresponding paper ballot.

1.1.6-D – Overvotes, undervotes, blank ballots

Voter-facing scanners must provide a function that can be activated by election officials to stop the scanning process and display a message which will enable the removal and correction of the ballot in response to the following ballot conditions:

1. ballots containing overvotes in a designated contest;
2. ballots containing undervotes in a designated contest;
3. ballots containing contests that were not voted; and
4. blank ballots.

Related requirements: 7.3-H – Overvotes
7.3-I – Undervotes

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000219

1.1.6-E – Write-ins, Ballot handling for vote-capture devices

Voter-facing scanners, when scanning a ballot containing a write-in vote, must either:

1. segregate the ballot in a manner that facilitate its later identification; or
2. if the ballot image uniquely identifies its corresponding ballot, use electronic adjudication to segregate the ballot.

Discussion

The requirement to separate ballots containing write-in votes is not applicable to systems in which a BMD encodes write-in votes in a machine-readable form. In this instance, and a scanner generates individual tallies for all written-in candidates automatically. Separation of ballots containing write-in votes is only necessary in systems that require the allocation of write-in votes to specific candidates to be performed manually.

1.1.6-F – Ability to clear mis-fed ballots

If multiple feed or misfeeding (jamming) occurs, batch-fed scanners must:

1. permit the operator to remove the ballots causing the error and reinsert them in the input hopper (if unread) or insert them in the ballot box (if read); and
2. prevent duplicate scanning of the ballots.

Discussion

Number 2 deals with whether CVRs have been created for the ballots that were jammed.

1.1.6-G – Scan to manufacturer specifications

The voting system must have the capability to provide a report of the mark detection thresholds that have been used to program the scanner so that the information is available upon request.

Discussion

Manufacturers must not make their specifications proprietary; auditors must be able to understand what and what does not constitute a valid voter mark on a particular scanner.

1.1.6-H – Accurately detect imperfect marks

The voting system must detect a *1 mm thick line* that:

1. is made with a #2 pencil that crosses the entirety of the contest option position on its long axis;

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000220

2. is centered on the contest option position; and

3. is as dark as can practically be made with a #2 pencil.

Discussion

Different optical scanning technologies will register imperfect marks in different ways. Variables include:

- the size, shape, orientation, and darkness of the mark;
- the size, shape, orientation, and darkness of the mark;
- the location of the mark within the voting target;
- the wavelength of light used by the scanner;
- the size and shape of the scanner's aperture;
- the color of the ink;
- the sensed background-white and maximum-dark levels; and
- the calibration of the scanner.

The mark specified in this requirement is intended to be less than 100 % perfect, but reliably detectable. In plain language: scanning technologies may vary, but as a minimum requirement, all of them should be capable of reliably reading *this* mark.

1.1.6-I – Ignore extraneous marks inside voting targets

The voting system must include a capability to recognize any imperfections in the ballot stock, folds, and similar insignificant marks appearing inside the voting targets and not record them as votes.

Discussion

Insignificant marks appearing inside of the voting targets could be detected as votes, thus the capability to recognize the ballot folds or imperfections must be included as a part of the voting system. It may not be possible to completely eliminate this problem in all cases depending on scanner thresholds for detecting marks.

Related requirements: 1.1.6-G – Scan to manufacturer specifications

1.1.6-J – Marginal marks, without bias

The detection of marginal marks from manually marked paper ballots must not show a bias.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000221

Discussion

Bias errors are not permissible in any system. An example of bias would be if marginal marks in the first ballot position were detected differently than marginal marks in the second ballot position.

1.1.6-K – Repeatability

The determination of a vote on a manually marked paper ballot must be repeatable, such that it never changes from a vote to a non-vote or from non-vote to a vote.

Discussion

Since it is technically impossible to achieve repeatable readings of ballots containing marks that fall precisely on the scanning threshold, changing between a non-vote and a marginally machine-readable mark is allowed. Similarly, changing from a valid vote and a marginally machine-readable mark is allowed.

1.1.7 – Exiting or suspending voting

1.1.7-A – Exiting or suspending election mode

The voting system must provide designated functions for exiting or suspending an election mode in which voting is permitted.

Discussion

When voting is conducted across multiple days, for example, during early voting, these requirements are still applicable even though the election itself may not be over; this is with the exception of requirement *1.1.7-E – Prevent re-entering election mode*, which deals with preventing re-opening of the polls once they have been closed on election day.

1.1.7-B – No voting when voting is stopped

The voting system must prevent the further activation, marking, or casting of ballots by any device once the voting has stopped.

Discussion

This requirement is applicable to voter-facing scanners, batch-fed scanners and any other device that enables the activation or tabulation of the voting process. However, a BMD cannot prevent a voter from marking a paper ballot with a writing utensil after polls have closed. This needs to be prevented through jurisdictional procedure.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000222

1.1.7-C – Voting stop integrity check

The voting system must provide an internal test that verifies that the prescribed closing or suspension procedures have been followed.

1.1.7-D – Report on voting stop process

The voting system must provide a means to produce a diagnostic test record that verifies the sequence of events, which indicate that the voting mode has been deactivated or suspended.

1.1.7-E – Prevent re-entering election mode

The voting system must not be capable of re-entering an election mode, in which voting is permitted, once the closing procedures have been completed for an election without an explicit override authorized by an administrator.

Discussion

When early voting is conducted across multiple days, this requirement does not prevent reopening of the polls on the following day.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations

1.1.8 – Tabulation

1.1.8-A – Tabulation

The voting system must support the tabulation function for all voting variations indicated in the implantation statement. This function includes:

1. extracting the valid votes from each ballot cast according to the defined rules;
2. creating and storing a CVR that contains the disposition of each contest selection as well as the disposition of each contest choice that is eligible to be cast; and
3. accumulation and aggregation of contest results and ballot statistics.

Discussion

Results accumulation and aggregation takes place at multiple levels within the voting system. Each tabulation unit must perform this function and must have the ability to transmit the CVRs and results to the election management system (EMS) for jurisdiction wide accumulation and aggregation.

AMERICAN OVERSIGHT

1.1.8-B – Partisan primary elections

In partisan primary elections, the voting system must be capable of reporting separate totals for the number of ballots read and the number of ballots counted for each political party. This is independent of whether the primary type is closed or open.

Discussion

From a tabulation perspective, there are two types of partisan primary election ballots. A *closed primary ballot* is one in which a ballot is limited to contests associated with one political party and any nonpartisan contests. An *open primary ballot* is one which contains contests from all parties on the same ballot, but the voter may only select contest choices applicable to a single party.

1.1.8-B.1 – Tabulation of a closed primary ballot

The voting system must support the tabulation of ballots that are specific to a party or are nonpartisan and must be able to report combined totals for nonpartisan contests no matter what party ballot the contest appears on.

1.1.8-B.2 – Tabulation of an open primary ballot

When tabulating ballots from an open primary, the voting system must limit tabulation of votes to contests of one political party.

Discussion

In an open primary, a voter may select partisan contest choices that are associated with more than one political party. Therefore, tabulation of a ballot during an open primary will void the partisan content of the ballot and only contest selections in nonpartisan contests are tabulated. The ballot is treated like a nonpartisan ballot.

1.1.8-B.3 – Open primary ballot with party preference contest

If the ballot contains a party preference contest and a party preference contest choice is selected, the voting system must only tabulate partisan contest option selections from contests that are of the same party as is selected in the party preference contest.

Discussion

A party preference contest provides the voter with the ability to select their intended party and avoid cross-party selections voiding the partisan selection of the ballot. If a party preference contest option is not selected, partisan contests on the ballot are tabulated as if the party preference contest was not present.

Related requirements: 1.1.4-N – Party preference contest

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000224

1.1.8-C – Write-ins, Tabulation

The voting system must be capable of

1. tabulating votes for write-in candidates with separate totals for each contest choice, and
2. tabulating valid individual write-in candidate totals in each contest.

Discussion

Tabulation of candidate names that are manually written in on a hand voted paper ballot can only be tabulated as an aggregate total in each contest. Each name must be adjudicated from graphical images of the contest write-in area or from the ballot itself to determine the name of the candidate. When names are typed on an electronic voting unit such as a BMD, although the entered names must be recorded, only aggregate contest write-in totals are tabulated. Each individual write-in name must be adjudicated for validity before they can be aggregated. In most states, a write-in candidate must be registered to be valid. State rules also determine acceptable variations in the written name for the candidate to be credited with the vote. State rules also determine treatment of a written-in name of a candidate already listed on the ballot.

1.1.8-D – Ballot rotation, Tabulation

When the order of contest choices within a contest varies by ballot style, the voting system must tabulate votes for each contest selection independent of a contest selections location in the contest on the ballot.

Discussion

This means that ballot rotation will not impact the correctness of the count.

1.1.8-E – Straight-party voting, Tabulation

When tabulating a partisan general election ballot, which includes a validly selected straight-party contest option in a straight-party contest, the voting system must select each candidate contest choice that is endorsed by the selected party in every contest on the ballot unless the contest is specifically exempted.

Discussion

There are currently two different tabulation rule sets for handling a ballot with both a straight-party selection and a selection in a contest of a candidate not endorsed by the selected party, known as party crossover. In one, any selection of a contest choice in a partisan contest eliminates any straight-party selection in that contest. In the other, straight-party option selections in a contest are eliminated if the number of candidates selected exceeds the allowed number, whether directly selected by the voter or automatically selected by the straight-party. Other rules are possible as well.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000225

Note that some states explicitly indicate that certain contests will not be affected by a straight-party selection.

1.1.8-F – Cross-party endorsement with straight-party voting

For straight-party tabulation, if a listed candidate option is endorsed by more than one political party, the voting system must be capable of tabulating votes for that candidate independent of which party option is validly selected.

1.1.8-G – Precinct splits, Tabulation

When multiple ballot styles are associated with a specific precinct, the voting system must be capable of keeping separate totals for the number of ballots read and counted for each ballot style or split. Tabulation must not be affected by variation of contest selection locations from one ballot style to another.

1.1.8-H – N-of-M contest, Tabulation

For N-of-M voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter is permitted to select up to a specified number of contest choices.

Discussion

An N-of-M contest is one where a voter is allowed *N contest selections* from a list of *M choices* and where votes are tallied independent of any other contest choices. N includes 1 vote (1 vote for 1 contest or typically a measure) or any larger number. Contest choices include those where the contest choices are candidates for a specific office or measures/referenda where there are usually only two contest choices (Yes/No, For/Against) but may also be a list of choices (Tax rate A, Tax rate B, Tax rate C). An N-of-M contest is used for *approval voting* by setting N to be equal to M. This type of contest is used for *limited voting* by setting N to be less than the number of seats being elected. An N-of-M contest is also is used for top-2 primary contests (blanket primary contests), where N is always 1 but the 2 candidates with the most votes will be on the general election ballot.

1.1.8-I – Cumulative voting contest, Tabulation

For cumulative voting, the voting system must be capable of tabulating votes, overvotes, and undervotes in contests where the voter may allocate up to a specified number of votes over a list of contest choices in any manner they choose. This may result in possibly giving more than one vote to a given contest selection.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000226

1.1.8-J – Ranked choice voting contest, Tabulation

For ranked choice voting (RCV), the voting system must

1. capture the voter's ranking of each contest selection and store it in the CVR associated with the ballot style;
2. aggregate 1st choice totals of each contest selection; and
3. process the collection of CVRs round-by-round according to the method specified in the implementation statement.

Discussion

Ranked choice voting (RCV) tabulation methods are different for single seat and multi-seat contests. Jurisdictional rules vary even when using the same basic method. A voting unit or precinct tabulating unit cannot perform RCV tabulation. RCV tabulation requires the concurrent availability of all CVRs associated with an RCV contest and is a post-voting accumulation/aggregation process. Some jurisdictional rules may only require use of the RCV tabulation process if aggregated first choice selections do not produce the total needed to exceed the threshold of votes required to win. Other jurisdictional rules do not use tabulated and aggregated 1st choice selections and require the RCV tabulation process to be used for all winners. Single winner RCV is also known as IRV (Instant Runoff Voting). STV (Single Transferable Vote) is a method used for multi-winner RCV. Another multi-winner process (Sequential At-Large IRV) uses successive IRV passes, one pass to determine each winner.

1.1.8-K – Group voting contest, Tabulation

When tabulating group voting contest choices, the voting system must automatically select each contest choice that is affiliated with the selected group as if the voter manually selected each of those candidate choices. Any selection of a contest choice outside of the group will constitute as an overvote if the number of candidates in the group selected is equal to the votes allowed.

Discussion

There may be multiple candidate groups in a contest. The ballot normally places contest options for all candidates in a group sequentially, with the group contest option first. If a contest is not fully voted by utilizing the group voting contest option, a voter can select additional contest options outside of the group, as long as the total does not exceed the votes allowed.

1.1.8-L – Presidential delegate contest, Tabulation

When tabulating a presidential delegate contest, the voting system must prevent votes for any delegate in the contest that is not representing the president candidate chosen by the voter's contest option selection in the presidential contest.

AMERICAN OVERSIGHT

Discussion

Most states that directly elect presidential delegates do not have a tabulation associated with the presidential candidate selection. However, as of 2020, Alabama has included this association on both the democratic and republican ballots, while Rhode Island has the association on the democratic ballot. When used, if there is no presidential candidate selection or the presidential candidate and no affiliated delegate in the contest, no vote will be counted for any delegate contest option selection.

1.1.8-M – Recall contest pair

When tabulating a recall/replace contest pair, the voting system must only tabulate the replace contest (controlled contest) if there is a vote selection in the recall contest (controlling contest).

Discussion

The *recall contest* in the contest pair is typically a question used to determine whether an elected official should be recalled and the replace contest allows selection of the desired replacement. If the question is not voted, the replacement contest is not processed. However, the contest pair has been used for other purposes such as annexations and determination of tax rates.

1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation

Votes selections in a proportional voting contest (also known as an equal-and-even cumulative voting contest) must be tabulated for the selected contest option or options by dividing the allowed votes by the number of contest option selections; this may occur as long as the number of selections do not exceed the number of allowed votes.

Discussion

This may produce a fractional number of votes tabulated for a candidate. However, it is not possible to tabulate undervotes in this contest.

1.1.9 – Reporting results

1.1.9-A – Post-election reports

The voting system must have the capability to create post-election reports that contain cast ballot counts and vote counts for contests on the ballot types served by precincts or splits of precincts.

AMERICAN OVERSIGHT

1.1.9-B – Report categories of cast ballots

The voting system must have the capability to report the number of ballots cast in total and broken down by ballot style. This is in addition to the associated units of political geography for the following categories of ballots cast:

1. All read ballots and all counted ballots,
2. For multi-page ballots, the number of different pages read, and number counted,
3. Read ballots and counted ballots that require review,
4. Absentee read and counted ballots, and
5. Blank ballots (ballots containing no votes).

Discussion

Associated units of political geography may also include state, county, city, town or township, ward, and districts.

1.1.9-C – Report categories of votes

The voting system must have the capability to report the following categories of votes:

1. in-person voting,
2. absentee voting,
3. write-ins,
4. accepted reviewed ballots, and
5. rejected reviewed ballots.

1.1.9-D – Reporting combined or split precincts

The voting system must be capable of generating reports that consolidate vote data from selected precincts.

Discussion

Jurisdictions in which more than one precinct may vote at the same location on either the same ballot style or a different ballot style may desire reports that consolidate data from the voting location by precinct.

AMERICAN OVERSIGHT

1.1.9-E – Report counted ballots by contest

The voting system must have the capability to report the number of counted ballots for each relevant N-of-M or cumulative voting contest.

Discussion

The count by contest could be inferred from the other counts that are broken down by ballot configuration, but providing this figure explicitly will make it easier to account for every vote. N-of-M in this requirement includes the most common type of contest, 1-of-M.

1.1.9-F – Report votes for each contest option

The voting system must have the capability to report the vote totals for each contest option in each relevant N-of-M or cumulative voting contest.

Discussion

N-of-M in this requirement includes the most common type of contest, 1-of-M.

1.1.9-G – Report overvotes for each contest

The voting system must have the capability to report the number of overvotes for each relevant N-of-M or cumulative voting contest.

1.1.9-H – Report undervotes for each contest

The voting system must have the capability to report the number of undervotes for each relevant N-of-M or cumulative voting contest.

Discussion

Counting ballots containing undervotes instead of votes lost to undervoting is insufficient.

1.1.9-I – Ranked choice voting, report results

The voting system must have the capability to report the contest choice vote totals for each ranked choice contest and for each round of tabulation.

Discussion

This requirement is minimal. Since ranked choice voting is not currently in wide use, it is not clear what needs to be reported, how bogus orderings are reported, or how it would be done in multiple reporting contexts.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000230

1.1.9-J – Precinct reporting devices, reporting device consolidation

When more than one vote-capture device is used in a polling place, the voting system must have the capability to consolidate the data tabulated by each unit into a single report for the polling place.

Discussion

This requirement essentially requires precinct-based vote-capture devices to be able to consolidate voting data for the purposes of issuing one consolidated report.

1.1.9-K – Precinct reporting devices, no tallies before polls close

The voting system must prevent the printing of vote data reports and extracting vote tally data while the polls are open.

Discussion

Providing ballot counts does not violate this requirement. The prohibition is against providing vote totals for ballot contests.

1.1.9-L – Report read ballots by party

The voting system must have the capability of reporting separate totals for each party in primary elections when reporting categories of read and counted cast ballots.

1.1.9-M – Reports are time stamped

All reports must include the date and time of the report's generation, including hours, minutes, and seconds.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000231

1.2 – The voting system is designed to function correctly under real-world operating conditions.

Requirements in this section deal with voting system accuracy and reliability.

1.2-A – Assessment of accuracy

The voting system's accuracy must be assessed by using a combination of evidence items gathered during the entire course of testing, including:

1. A measurement of how accurately voter marks are recognized as valid or not valid according to manufacturer specifications.
2. A measurement of how accurately voter marks are tabulated and reported as results.
3. An assessment of whether the remaining VVSG requirements are satisfied.

Discussion

The data collected during the testing of this requirement contributes substantially to the evaluations of reliability, accuracy, and misfeed rate.

1.2-B – Reliably detectable marks

The voting system must detect marks on the ballot consistent with system mark specifications and differentiate between voter-made marks constituting votes versus voter-made marginal marks or other marks on the ballot.

Discussion

The specification may have parameters for different configuration values. It should also state the degree of uncertainty.

1.2-C – Minimum ballot positions

A minimum of 10,000,000 ballot positions must be read by the voting system and tabulated accurately.

Discussion

The value of 10,000,000 ballot positions is taken from *VVSG 1.0 [VVSG2005]*, however it is used here as the minimum number of ballot positions to test without error. If a larger number of ballot positions is used, there still can be no error.

AMERICAN OVERSIGHT

1.2-D – Handle maximum volume

The voting system must be able to handle the maximum volume of activities in conditions approximating normal use in an entire election process according to manufacturer specifications.

Discussion

This requirement should be verified through operational testing if the limit is practically testable.

1.2-E – Respond gracefully to stress of system limits

Certain conditions tend to overload the system's capacity to process, store, or report data. These conditions include attempts to process more than the expected number of precincts, and to process more than the expected volume or ballot tabulation rate. Therefore, the voting system must be able to respond to the above conditions that overload the system's capacity, by ensuring that the voting system does not fail or halt suddenly. The voting system must give adequate warning if it is to fail or halt for any reason.

Discussion

This requirement should be verified through operational testing if the limit is practically testable.

1.2-F – No single point of failure

The voting system must protect against a single point of failure that would prevent further voting at the polling place.

Discussion

The intent of this requirement is to prevent, at the polling place, a situation in which failure of a component would prevent voting. This can be addressed in various ways, including being able to swap in/out devices without loss of data.

1.2-G – Misfeed rate benchmark

The voting system misfeed rate must not exceed 0.002 (1 / 500).

Discussion

Multiple feeds, misfeeds (jams), and rejections of ballots that meet all manufacturer specifications are all treated collectively as "misfeeds" for benchmarking purposes; that is, only a single count is maintained.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000233

1.2-H – Protect against failure of input and storage devices

The voting system must withstand, without loss of data, the failure of any data input or storage device.

Discussion

The intent of this requirement is to prevent votes from being permanently lost due to the failure of a storage device that contains votes. For example, if a scanner fails, the voting system must have the ability to swap in a replacement data input device without the losing cast vote records that were previously recorded by the failed scanner.

1.2-I – FCC Part 15 Class A and B conformance

Voting devices must comply with the requirements of the *Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]*.

1. Voting devices located in polling places must minimally comply with Class B requirements.
2. Voting devices located in non-polling place settings such as back offices must minimally comply with Class A requirements.

1.2-J – Power supply from energy service provider

Voting devices located in polling places must be powered by a 120 V, single phase power supply derived from typical energy service providers.

Discussion

It is assumed that the AC power necessary to operate the voting system will be derived from the existing power distribution system of the facility housing the polling place. This single-phase power may be a leg of a 120/240 V single phase system, or a leg of a 120/208 V three-phase system, at a frequency of 60 Hz.

1.2-K – Power port connection to the facility power supply

Voting devices located in polling places must comply with Class B emission limits affecting the power supply connection to the energy service provider.

Discussion

The normal operation of an electronic system can produce disturbances that will travel upstream and affect the power supply system of the polling place, creating a potential deviation from the expected electromagnetic compatibility of the system. The issue is whether these actual disturbances (after

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000234

possible mitigation means incorporated in the equipment) reach a significant level to exceed stipulated limits.

1.2-L – Leakage from grounding port

Voting devices located in polling places must comply with limits of leakage currents effectively established by the trip threshold of all listed Ground Fault Current Interrupters (GFCI), if any, installed in the branch circuit supplying the voting system.

Discussion

Excessive leakage current is objectionable for two reasons:

- For a branch circuit or wall receptacle that could be provided with a GFCI (depending upon the wiring practice applied at the particular polling place), leakage current above the GFCI built-in trip point would cause the GFCI to trip and therefore disable the operation of the system.
- Should the power cord lose the connection to the equipment grounding conductor of the receptacle, a personnel hazard would occur. (Note the prohibition of "cheater" adapters in the discussion of general requirements for the polling place.)

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000235

1.3 – Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

1.3-A – Reporting of manufacturer-performed tests

Each test provided in a manufacturer-submitted report of internal testing performed (technical data package (TDP)) must, at least, include the following information:

1. requirement(s) under test;
2. items under test to exercise a given requirement;
3. pass-fail criteria necessary to determine whether or not a requirement has passed the test of conformity to the requirement;
4. evidence (observations, data) expected to provide justification for satisfying or failing a given pass-fail condition;
5. test procedures necessary to provide, observe, record, analyze, and interpret this evidence relative to pass-fail criteria;
6. where applicable, descriptions of the causes of variation, ambiguity, noise, or observed errors in observed and recorded evidence during tested procedures;
7. where applicable, descriptions of any necessary techniques, procedures, or processes applied to normalize or clean data prior to subjecting it to data analysis and interpretation relative to pass-fail criteria;
8. report of actual tests performed and their results; and
9. description and justification if a given test cannot be fully performed or exercised due to internal resource constraints, including description of alternative means of verification.

Discussion

This is a documentation requirement. Its intent is to ensure a baseline set of information provided in manufacturer-submitted report of manufacturer-performed internal testing submitted as part of the TDP. Manufacturers may likely have additional information, formatting, etc., as part of their particular testing practices, that they will include as is consistent with their internal testing best-practices.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000236

1.3-B – Coverage of manufacturer-performed tests

Each requirement identified in a manufacturer-submitted implementation statement or conformance statement must describe one-or-more tests in their test-plan describing how it was tested.

Discussion

This requirement is to ensure that all requirements identified in the respective implementation and conformance statements are covered by the submitted test-plan.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000237

Principle 2
High Quality Implementation

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

2.2 - The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.4 - Voting system structure is modular, scalable, and robust.

2.5 – The voting system supports system processes and data with integrity.

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.7 - The voting system performs reliably in anticipated physical environments.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000238

Principle 2
High Quality Implementation

The voting system is implemented using high quality best practices. are designed to provide transparency.

This principle covers core processes and functions that contribute to a voting system that has been implemented for quality. The requirements in this principle are basic best practices -- not a complete set of all quality practices. The guidelines under *Principle 2* are:

2.1 - **Software quality**, including acceptable programming languages and coding styles, as well as coding constructs that should or should not be used to improve software integrity and security. Additional requirements deal with handling errors or device failures, and others cover electrical components. The sections in ***Guideline 2.1*** cover:

1 – Workmanship which deals with best practices for providing high quality systems and parts, taking reasonable precautions to prevent defect or damage, and ensuring that system elements can be sufficiently durable and available with respect to lifetimes that are appropriate to their type and use.

2 – Maintainability covers the ability of a system and its components to be sufficiently identified and repaired during its operational lifetime.

2.2 - **Design and implementation process** so that the voting system can be used effectively by voters and election staff.

2.3 - Voting system logic or the overall structuring of voting system software. The goal is that the software structure be easily understood and clear to audiences such as test labs and maintained without causing major changes in the software structure. The sections in ***Guideline 2.3*** cover:

1 – Software flow which identifies common pitfalls to be avoided when organizing software control flow so as to preserve its clarity and ease of evaluation.

2.4 - **Modularity** and complexity of the system software structure.

2.5 - System processes and data using basic best practices for software integrity and secure coding constructs. The Election Assistance Commission (EAC), working with voting system test labs, may augment or change these requirements based on the discovery of new vulnerabilities or emerging new threats. The sections in ***Guideline 2.5*** cover:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000239

1 – Code integrity which deals with the protection of code from unauthorized change or tampering.

2 – Input/output errors supports practices to ensure the validity of inputs and outputs while also guarding against associated errors.

3 – Output protection which deals with the ability to protect against vulnerabilities known to affect outputs.

4 – Error handling addresses the need for internal error checking, particularly for common types of coding errors such as various types of overflows, pointer-related errors, and so on.

2.5 and 2.6 - **Graceful recovery** the capability of the voting system to handle and recover from errors, including failures of devices and components.

2.7 - **Physical environments** includes the ability of a voting device to withstand influences from its physical environment whether due to humidity, temperature, shock, vibration, electrical, or related influences.

The requirements on electrical disturbances are primarily covered by conformance to the *Rules and Regulations of the Federal Communications Commission, Part 15, Class B [FCC19a]*. The requirements here address items not covered by Class B, including the behavior of specific voting devices in the presence of electrical disturbances and cases where voting devices might interact with other devices or people.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000240

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

2.1-A – Acceptable programming languages

Application logic must be produced in a high-level programming language that has all of the following control constructs:

1. sequence;
2. loop with exit condition (for example, for, while, or do-loops);
3. if/then/else conditional;
4. case conditional; and
5. block-structured exception handling (for example, try/throw/catch).

Discussion

A list of acceptable programming languages may be specified by the EAC in conjunction with voting system test labs.

This requirement can be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform.

By excluding border logic, this requirement allows the use of assembly language for hardware-related segments, such as device controllers and handler programs. It also allows the use of an externally imposed language for interacting with an Application Program Interface (API) or database query engine. However, the special code should be insulated from the bulk of the code, for example, by wrapping it in callable units expressed in the prevailing language to minimize the number of places that special code appears.

Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions (*[VVSG2005] I.5.2.3.e*), but there was no unambiguous requirement for the programming language to support exception handling. These guidelines require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked. Additionally, these guidelines require block-structured exception handling because, like all unstructured programming, unstructured exception handling obfuscates logic and makes its verification by the test lab more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide.

AMERICAN OVERSIGHT

This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software." *[Moulding89]*

Existing voting system logic implemented in programming languages that do not support block-structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this (see Requirement *2.1-B – COTS language extensions are acceptable*).

2.1-B – COTS language extensions are acceptable

Requirement *2.1-A – Acceptable programming languages* may be satisfied by using COTS extension packages to add missing control constructs to languages that could not otherwise conform.

Discussion

The use of non-COTS extension packages or manufacturer-specific code for this purpose is not acceptable, as it would place an unreasonable burden on the test lab to verify the soundness of an unproven extension (effectively a new programming language). The package must have a proven track record of performance supporting the assertion that it would be stable and suitable for use in voting systems, just as the compiler or interpreter for the base programming language must.

2.1-C – Acceptable coding conventions

Application logic must adhere to a published, credible set of coding rules, conventions, or standards (called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications.

Discussion

Coding conventions may be specified by the EAC in conjunction with voting system test labs.

The requirement to follow coding conventions serves two purposes. First, by requiring specific risk factors to be mitigated, coding conventions support integrity and maintainability of voting system logic. Second, by making the logic more transparent to a reviewer, coding conventions facilitate test lab evaluation of the logic's correctness to a level of assurance beyond that provided by operational testing.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000242

The source code review for workmanship now focuses on coding practices with a direct impact on integrity and transparency and on adherence to published, credible coding conventions, in lieu of coding conventions embedded within the standard itself.

The vast majority of coding conventions used in practice are tailored to specific programming languages. In these guidelines, the few coding conventions that have significant impact on integrity and transparency and that generalize relatively well to different programming languages have been retained, expanded, and made mandatory, while the many coding conventions that are language sensitive and stylistic in nature, and are made redundant by more recent, publicly available coding conventions, have been removed in favor of the published conventions.

As discussed, prescriptive coding conventions not directly related to integrity and transparency have been avoided in favor of published, credible conventions.

Coding conventions are considered to be **published** if they appear in a publicly available book, magazine, journal, or new media with analogous circulation and availability, or if they are publicly available on the Internet. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged.

Coding conventions are considered to be **credible** if at least two different organizations with no ties to the creator of the rules or to the manufacturer seeking conformity assessment, and which are not themselves voting equipment manufacturers, independently decided to adopt them and made active use of them at some point within the three years before conformity assessment was first sought. This requirement attempts to clarify the "published, reviewed, and industry-accepted" language appearing in previous iterations of the VVSG, but the intent of the requirement is unchanged.

Coding conventions evolve, and it is desirable for voting systems to be aligned with modern practices.

2.1-D – Records last at least 22 months

All systems must maintain the integrity of election management, voting, and audit data, including cast vote records (CVRs), during an election and for a period of at least 22 months afterward, in temperatures ranging from 5 C to 40 C (41 F to 104 F) and relative humidity from 5% to 85%, non-condensing.

2.1.1 – Workmanship

2.1.1-A – General build quality

All manufacturers of voting systems must practice proper workmanship by:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000243

1. adopting and adhering to practices and procedures that ensure their products are free from damage or defect that could make them unsatisfactory for their intended purpose; and
2. ensuring that components provided by external suppliers are free from damage or defect that could make them unsatisfactory or hazardous when used for their intended purpose.

2.1.1-B – Durability estimation

A manufacturer must submit a warranty model to the EAC, testing labs, and customers, that includes for each product, its relevant components, and associated consumables:

1. estimated replacement rates (e.g., 3 years, 10 years);
2. estimated costs per replacement;
3. estimated warranty types and costs;
4. associated replacement policies, services, and available maintenance agreements; and
5. plans for collecting, maintaining, and reporting data to the EAC to support and validate estimates.

Discussion

A number of factors associated with the durability of a product or its components can be highly variable and even particular to the type of components (e.g., COTS, consumables). This variance is also applicable to the resources of a given manufacturer. Thus, instead of prescribing a pre-estimated number for all manufacturers, the manufacturers are asked to make these estimates relative to their own products, components, and resources, and to provide the basis for these estimates (these warranties, replacement periods, etc.) to the EAC, labs, and customers. In this way, manufacturers can perform estimates most relevant to their chosen manufacturing strategies (i.e., COTS-centric vs. custom-built, and so on).

2.1.1-C – Durability of paper

Paper specified for use with the voting system must conform to the applicable specifications contained within the *Government Paper Specification Standards, February 1999 No. 11*, or the government standards that have superseded them.

Discussion

This is to ensure that paper records will be of adequate quality to survive the handling necessary for recounts, audits, etc. without problematic degradation. The Government Paper Specification

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000244

Standards include different specifications for different kinds of paper. As of 2020-02-29, the *Government Paper Specification Standards, February 1999 No. 11 [GPO19].*

2.1.1-D – Ensure compatibility of specified paper and ink

Ink specified for use with the voting system must be compatible with the paper specifications provided by the manufacturer.

Discussion

The purpose of this requirement is to ensure that both the types of ink and paper used with a given system are compatible with each other in an effort to avoid many of the side-effects of mismatched ink and paper (e.g., excessive smudging).

2.1.2 – Maintainability

2.1.2-A – Electronic device maintainability

Electronic devices must exhibit the following physical attributes:

1. labels and the identification of test points;
2. built-in test and diagnostic circuitry or physical indicators of condition; and
3. labels and alarms related to failures.

2.1.2-B – System maintainability

Voting systems must allow for:

1. a non-technician to easily detect that the equipment has failed;
2. a trained technician to easily diagnose problems;
3. easy access to components for replacement;
4. easy adjustment, alignment, and tuning of components; and
5. low false alarm rates (that is, indications of problems that do not exist).

2.1.2-C – Nameplate and labels

All voting devices must:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000245

1. Display a permanently affixed nameplate or label containing the name of the manufacturer, the name of the device, its part or model number, its revision identifier, its serial number, and if applicable, its power requirements.
2. If service or preventative maintenance is required, display a separate data plate containing a schedule for and list of operations required to service or to perform preventive maintenance, or a reference to where this can be found in the voting equipment user documentation.
3. Display advisory caution and warning instructions to ensure safe operation of the equipment and to avoid exposure to hazardous electrical voltages and moving parts at all locations where operation or exposure may occur.

2.2 – The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.2-A – User-centered design process

The manufacturer must submit a report providing documentation that the system was developed following a user-centered design process.

The report must include, at a minimum:

1. a listing of user-centered design methods used;
2. the types of voters and election workers included in those methods;
3. how those methods were integrated into the overall implementation process; and
4. how the results of those methods contributed to developing the final features and design of the voting system.

Discussion

The goal of this requirement is to allow the manufacturer to demonstrate, through the report, the way their implementation process included user-centered design methods.

ISO-9241-210:2019 Ergonomics of human-system interaction—Part 210: Human-centered design for interactive systems [ISO19b] provides requirements and recommendations for human-centered principles and activities throughout the life cycle of computer-based interactive systems. It includes

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000246

the idea of iterative cycles of user research to understand the context of use and user needs, creating prototypes or versions, and testing to confirm that the product meets the identified requirements.

This requirement does not specify the exact user-centered design methods to be used, or their number or timing.

The ISO group of requirements, S*oftware engineering -- Software product Quality Requirements and Evaluation (SQUARE) -- Common Industry Format (CIF) for Usability* includes several standards that are a useful framework for reporting on user-centered design activities and usability reports:

- *ISO/IEC TR 25060:2010: General framework for usability-related information [ISO10]*
- *ISO/IEC 25063:2014: Context of use description [ISO14]*
- *ISO/IEC 25062:2006: Usability test reports [ISO06b]*
- *ISO/IEC 25064:2013: User needs report [ISO13b]*
- *ISO/IEC 25066:2016 Evaluation report [ISO16]*

Related requirements: 8.3-A – Usability tests with voters
8.4-A – Usability tests with election workers

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.3-A – Block-structured exception handling

Application logic must handle exceptions using block-structured exception handling constructs.

Discussion

The concept of "block-structured exception handling," is the ability to associate exception handlers with blocks of logic, and implicitly, the presence of the exception concept in the programming language. (This simply means try/throw/catch or equivalent statements and should not be confused with the specific implementation known as Structured Exception Handling (SEH) [MS20].[2]) Unlike deeply nested blocks, exceptions cannot be eliminated by restructuring logic. "When exceptions are not used, the errors cannot be handled but their existence is not avoided." *[ISO00]*

Previous versions of VVSG required voting systems to handle such errors by some means, preferably using programming language exceptions ([*VVSG2005] I.5.2.3.e*), but there was no unambiguous requirement for the programming language to support exception handling. These guidelines require programming language exceptions because without them, the programmer must check for every possible error condition in every possible location, which both obfuscates the application logic and creates a high likelihood that some or many possible errors will not be checked. Additionally, these guidelines require block-structured exception handling because, like all unstructured programming,

AMERICAN OVERSIGHT

unstructured exception handling obfuscates logic and makes its verification by the test lab more difficult. "One of the major difficulties of conventional defensive programming is that the fault tolerance actions are inseparably bound in with the normal processing which the design is to provide. This can significantly increase design complexity and, consequently, can compromise the reliability and maintainability of the software." *[Moulding89]*.

2.3-B – Legacy library units

If application logic makes use of any COTS or third-party logic callable units that do not throw exceptions when exceptional conditions occur, those callable units must be wrapped in callable units that check for the relevant error conditions and translate them into exceptions, and the remainder of application logic must use only the wrapped version.

Discussion

Existing voting system logic implemented in programming languages that do not support block structured exception handling can be brought into compliance either through migration to a newer programming language (most likely, a descendant of the same language that would require minimal changes) or through the use of a COTS package that retrofits block-structured exception handling onto the previous language with minimal changes. While the latter path may at first appear to be less work, it should be noted that many library functions may need to be adapted to throw exceptions when exceptional conditions arise, whereas in a programming environment that had exceptions to begin with the analogous library functions would already do this.

2.3-C – Separation of code and data

Application logic must not compile or interpret configuration data or other input data as a programming language.

Discussion

The applicable requirement in VVSG2005 reads "Operator intervention or logic that evaluates received or stored data must not re-direct program control within a program routine." That attempt to define what it means to compile or interpret data as a programming language caused confusion.

Distinguishing what is a programming language from what is not requires some professional judgment. However, in general, sequential execution of imperative instructions is a characteristic of conventional programming languages that should not be exhibited by configuration data. Configuration data must be declarative or informative in nature, not imperative.

For example: Configuration data can contain a template that informs a report generating application about the form and content of a report that it should generate. However, configuration data cannot contain instructions that are executed or interpreted to generate a report, essentially embedding the logic of the report generator inside the configuration data.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000248

The reasons for this requirement are

- mingling code and data is bad design, and
- embedding logic within configuration data evades the conformity assessment process for application logic.

2.3-D – Hard-coded passwords and keys

Voting system software must not contain hard-coded, including the use of:

1. passwords, or
2. cryptographic keys.

Discussion

Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at *MITRE CWE-259: Use of Hard-coded Password [MITRE20a]* and *MITRE CWE-321: Use of Hard-coded Cryptographic Key [MITRE20b].*

2.3.1 – Software flow

2.3.1-A – Unstructured control flow

Application logic must contain no unstructured control constructs.

Discussion

Although it is typically developed by the voting system manufacturer, border logic is constrained by the requirements of the third-party or COTS interface with which it interacts. It is not always possible for border logic to achieve its function while conforming to standard coding conventions. For this reason, border logic should be minimized relative to application logic and where possible, wrapped in a conforming interface. An example of border logic that could not be so wrapped is a customized boot manager that connects a bootable voting application to a COTS BIOS.

2.3.1-B – Goto

Arbitrary branches (also known as gotos) must not be used.

2.3.1-C – Intentional exceptions

Exceptions must only be used for abnormal conditions. Exceptions must not be used to redirect the flow of control in normal ("non-exceptional") conditions.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000249

"Intentional exceptions" cannot be used as a substitute for arbitrary branch. Normal, expected events, such as reaching the end of a file that is being read from beginning to end or receiving invalid input from a user interface, are not exceptional conditions and should not be implemented using exception handlers.

2.3.1-D – Unstructured exception handling

Unstructured exception handling (for example, On Error GoTo, setjmp/longjmp, or explicit tests for error conditions after every executable statement) is prohibited.

Discussion

The internal use of such constructs by a COTS extension package that adds block-structured exception handling to a programming language that otherwise would not have it, as described in requirement *2.3-B – Legacy library units*, is allowed. Similarly, it is not a problem that source code written in a high-level programming language is compiled into low-level machine code that contains arbitrary branches. It is only the direct use of low-level constructs in application logic that presents a problem.

2.4 - Voting system structure is modular, scalable, and robust.

2.4-A – Modularity

Application logic must be designed in a modular fashion, meeting all the criteria stated in the definition of a module, namely that:

1. It must be a structural unit of software or analogous logical design.
2. If it contains callable units, those callable units must be tightly coupled.
3. Coupling between modules (“inter-module coupling”) must:
    a. be loose, and
    b. occur over defined interfaces.
4. It must contain all elements needed to compile or interpret successfully.
5. It must have limited access to data in other modules.
6. It must be substitutable with another module whose interfaces match the original module.

Discussion

The modularity rules described here apply to the component submodules of a library.

AMERICAN OVERSIGHT

2.4-B – Module testability

Each module must have a specific function that can be tested and verified independently of the remainder of the code.

Discussion

In practice, some additional modules (such as library modules) can be needed to compile the module being tested, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.

2.4-C – Module size and identification

Modules must be small and easily identifiable, such as being:

1. no more than 50% of all callable units (functions, methods, operations, subroutines, procedures, etc.) SHOULD exceed 25 lines of code in length, excluding comments, blank lines, and initializers for read-only lookup tables;
2. no more than 5% of all callable units SHOULD exceed 60 lines in length; and
3. no callable units SHOULD exceed 180 lines in length.

Discussion

"Lines," in this context, are defined as executable statements or flow control statements with suitable formatting.

2.4-D – Large data structures in separate files

Read-only large data structures longer than 25 lines must be placed in separate files from other source code if the programming language permits it.

Discussion

In practice, this case has often been illustrated by the need to put read-only large lookup tables into separate files. However, the same notion could apply to other kinds of data structures.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000251

2.5 - The voting system supports system processes and data with integrity.

2.5-A – Self-modifying code

Application logic must not be self-modifying.

2.5-B – Unsafe concurrency

Application logic must be free of race conditions, deadlocks, livelocks, and resource starvation.

Discussion

In addressing this requirement, information should be provided in the TDP describing the means by which *safe concurrency* was ensured relative to the design, implementation, and testing of the application logic.

2.5.1 – Code integrity

2.5.1-A – COTS compilers

If compiled code is used, it must only be compiled using a COTS compiler.

Discussion

This prohibits the use of arbitrary, nonstandard compilers and, consequently, the invention of new programming languages.

2.5.1-B – Interpreted code, specific COTS interpreter

If interpreted code is used, it must only be run under a specific, identified version of a COTS runtime interpreter.

Discussion

This ensures that:

- no arbitrary, nonstandard interpreted languages are used, and
- the software tested and approved during the conformity assessment process does not change behavior because of a change to the interpreter.

AMERICAN OVERSIGHT

2.5.1-C – Prevent tampering with code

Programmed devices must prevent replacing or modifying executable or interpreted code (for example, by other programs on the system, by people physically replacing the memory or medium containing the code, or by faulty code) except where this access is necessary to conduct the voting process.

Discussion

This requirement can be satisfied through a combination of:

- read-only memory (ROM),
- the memory protection implemented by most popular COTS operating systems,
- error checking, and
- access and integrity controls.

2.5.1-D – Prevent tampering with data

All voting devices must prevent access to or manipulation of configuration data, vote data, or audit records (for example, by physically tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct the voting process.

Discussion

This requirement can be satisfied through a combination of:

- the memory protection implemented by most popular COTS operating systems,
- error checking, and
- access and integrity controls.

Systems using mechanical counters to store vote data need to protect the counters from tampering. If vote data are stored on paper, the paper needs to be protected from tampering. Modification of audit records after they are created is never necessary.

2.5.2 – Input/output errors

2.5.2-A - Input validation and error defense

The voting system must:

1. monitor I/O operations;
2. validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values;
3. report any input errors and how they were corrected; and

AMERICAN OVERSIGHT

4. check information inputs to ensure that incomplete or invalid inputs do not lead to irreversible error.

Discussion

Input includes data from any input source: input devices (such as touch screens, keyboards, keypads, optical/digital scanners, and assistive devices), networking port, data port, or file. This general requirement applies to all programmed devices, while the specific ones following are only enforceable for application logic.

2.5.3 – Output protection

2.5.3-A – Escaping and encoding output

Software output must be properly encoded, escaped, and sanitized.

Discussion

The output of a software module can be manipulated or abused by attackers in unexpected ways to perform malicious actions. Ensuring that outputted data is of an expected type or format assists in preventing this abuse. Additional information about this software weakness can be viewed at *MITRE CWE 116: Improper Encoding or Escaping of Output [MITRE20c].*

2.5.3-B – Sanitize output

The voting system must sanitize all output to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the output source.

Discussion

Output includes data to any output source: output devices (such as touch screens, LCD screens, printers, and assistive devices), networking port, data port, or file. This applies to all parts of the voting system including the election management system (EMS).

2.5.3-C – Stored injection

The voting system must sanitize all output to files and databases to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the voting system if the stored data is read or imported at a later date or by another part of the voting system.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000254

A stored injection attack saves malicious data which is harmless when stored, but which is potent when read later in a different context or when converted to a different format. For example, a malicious script might be written to a file and do no harm to the voting machine, but later be evaluated and harmful when the file is transferred and read by the EMS. Input should also be filtered, but sanitizing stored output provides defense in depth.

2.5.4 – Error handling

2.5.4-A – Mandatory internal error checking

Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur:

1. common memory management errors, such as out-of-bounds accesses of arrays, strings, and buffers used to manage data;
2. uncontrolled format strings;
3. CPU-level exceptions such as address and bus errors, dividing by zero, and the like;
4. variables that are not appropriately handled when out of expected boundaries;
5. numeric and integer overflows;
6. validation of array indices; and
7. known programming language specific vulnerabilities.

Discussion

Logic verification will show that some error checks cannot logically be triggered, and some exception handlers cannot logically be invoked. These checks and exception handlers are not redundant – they provide defense-in-depth against faults that escape detection during logic verification.

2.5.4-B – Array overflows

If the application logic uses arrays, vectors, or any analogous data structures, and the programming language does not provide automatic run-time range checking of the indices, the indices must be ranged-checked on every access.

Discussion

Range checking code should not be duplicated before each access. Clean implementation approaches include:

- consistently using dedicated accessors (such as functions, methods, operations, subroutines, and procedures) that range-check the indices;

AMERICAN OVERSIGHT

- defining and consistently using a new data type or class that encapsulates the range-checking logic;
- declaring the array using a template that causes all accessors to be range-checked; or
- declaring the array index to be a data type whose enforced range is matched to the size of the array.

Range-enforced data types or classes can be provided by the programming environment or they can be defined in application logic. If acceptable values of the index do not form a contiguous range, a map structure can be more appropriate than a vector.

2.5.4-C – Buffer overflows

If an overflow does not automatically result in an exception, the application logic must explicitly check for and prevent the overflow.

2.5.4-D – CPU traps

The application logic must implement such handlers as needed to detect and respond to CPU-level exceptions.

Discussion

For example, under Unix, a CPU-level exception would manifest as a signal, so a signal handler is needed. If the platform supports it, it is preferable to translate CPU-level exceptions into software-level exceptions so that all exceptions can be handled in a consistent fashion within the voting application. However, not all platforms support it.

2.5.4-E – Garbage input parameters

All scalar or enumerated type parameters whose valid ranges as used in a callable unit (such as function, method, operation, subroutine, and procedure) do not cover the entire ranges of their declared data types must be range-checked on entry to the unit.

Discussion

This applies to parameters of numeric types, character types, temporal types, and any other types for which the concept of range is well-defined. In cases where the restricted range is frequently used or associated with a meaningful concept within the scope of the application, the best approach is to define a new class or data type that encapsulates the range restriction, eliminating the need for range checks on each use.

This requirement deals with user input that is expected to contain errors. User input errors are a normal occurrence; the errors discussed here are grounds for throwing exceptions.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000256

2.5.4-F – Numeric overflows

If the programming language does not provide automatic run-time detection of numeric overflow, all arithmetic operations that could potentially overflow the relevant data type must be checked for overflow.

Discussion

Encapsulate overflow checking as much as possible.

2.5.4-G – Uncontrolled format strings

Voting system software must not contain uncontrolled format strings.

Discussion

Many examples of this vulnerability have previously been identified in voting system software. Additional information about this vulnerability can be found at *MITRE CWE 134: Use of Externally-Controlled Format String [MITRE20d].*

2.5.4-H – Recommended internal error checking

Application logic that is vulnerable to the following types of errors must check for these errors at run time and respond defensively when they occur:

1. pointer variable errors, and
2. dynamic memory allocation and management errors.

2.5.4-I – Pointers

If application logic uses pointers or a similar mechanism for specifying absolute memory locations, the application logic must validate these pointers or addresses before they are used.

Discussion

The goal is to prevent improper overwriting, even if read-only memory would prevent the overwrite from succeeding. An attempted overwrite indicates a logic fault that must be corrected.

Pointer use that is fully encapsulated within a standard platform library is treated as COTS software.

2.5.4-J – Memory mismanagement

If dynamic memory allocation is performed in application logic, the application logic must be able to be instrumented or analyzed with a COTS tool for detecting memory management errors.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000257

Discussion

Dynamic memory allocation that is fully encapsulated within a standard platform library is treated as COTS software.

2.5.4-K – Nullify freed pointers

If pointers are used, any pointer variables that remain within scope after the memory they point to is deallocated must be set to null or marked as invalid (pursuant to the idiom of the programming language used).

Discussion

If this is not done automatically by the programming environment, a callable unit should be dedicated to the task of deallocating memory and nullifying pointers. Equivalently, "smart pointers" like the C++ std::auto_ptr can be used to avoid the problem. One should not add assignments after every deallocation in the source code.

In languages using garbage collection, memory is not deallocated until all pointers to it have gone out of scope, so this requirement is moot.

2.5.4-L – React to errors detected

Detecting any of the errors enumerated in these requirements must be treated as a complete failure of the callable unit in which the error was detected.

1. An appropriate exception must be thrown, and
2. Control must pass out of the unit immediately.

2.5.4-M – Election integrity monitoring

Electronic devices must proactively detect or prevent basic violations of election integrity (for example, stuffing the ballot box or accumulating negative votes) and alert an election official or administrator if they occur.

Discussion

Equipment can only verify those conditions that are within the scope of what the equipment does. However, if the equipment can detect something that is blatantly wrong, it should do so and raise the alarm. This provides defense-in-depth to supplement procedural controls and auditing practices.

2.5.4-N – SQL injection

The voting system application must defend against SQL injection.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000258

Discussion

SQL injection is a classic type of software weakness still prevalent today. SQL injection is not just a web-based issue, as any application accepting untrusted user input and passing it to a database can be vulnerable. Additional information about this software weakness can be viewed at *MITRE CWE 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') [MITRE20e].*

2.5.4-O – Parameterized queries

Any structured statement or command being prepared using dynamic data (including user input) to be sent to a database or other process must parameterize the data inputs and apply strict type casting and content filters on the data (such as prepared statements).

Discussion

Parametrized queries are a common defense against this class of software weakness.

AMERICAN OVERSIGHT

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.6-A – Surviving device failure

All systems must be capable of resuming normal operation following the correction of a failure:

1. in any device;
2. in any component (for example, memory, CPU, ballot reader, or printer) provided that catastrophic electrical or mechanical damage has not occurred; and
3. in a controlled fashion so that system status can be restored to the initial state existing before the error occurred.

Discussion

"Initial state" refers to the state existing at the start of a logical transaction or operation. Transaction boundaries must be defined in a conscientious fashion to minimize the damage. The final state is optional because election officials responding to the error condition might want the opportunity to select a different state, such as a controlled shutdown with memory dump for later analysis.

2.6-B – No compromising voting or audit data

Exceptions and system recovery must be handled in a manner that protects the integrity of all recorded votes and audit log information.

2.6-C – Coherent checkpoints

When recovering from non-catastrophic failure of a device or from any error or malfunction that is within the operator's ability to correct, the system must restore the device to the last known good state existing immediately before the error or failure, without loss or corruption of voting data previously stored in the device.

Discussion

If the system is left in something other than the last known good state for diagnostic reasons, this requirement clarifies that it must revert to the last known good state before being placed back into service.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000260

2.7 - The voting system performs reliably in anticipated physical environments.

Requirements in this section deal with voting system reliability with regard to environmental conditions and electrical surges and interference.

2.7-A – Assessment of reliability

The voting system's reliability must be assessed using a combination of evidence items gathered during the entire course of testing, including:

1. continuous operation of the voting system under typical environmental conditions;
2. continuous operation of the voting system under varied environmental conditions across defined ranges; and
3. resistance of the voting system to electrical surges, interference, and loss of power.

Discussion

As with accuracy, reliability cannot be positively ascertained; a judgment of reliability has to be determined from evidence. In this case, a volume test *[CA06]* is used during various environmental conditions to determine the reliability of the voting system operations, as well as data from the test campaign regarding relevant VVSG requirements.

2.7-B – Continuous operation – typical environmental conditions

The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error.

2.7-C – Continuous operation – varied environmental conditions

The voting system must operate for a continuous period of time during which ballots are cast and ballot positions are read and tabulated without error and in which temperature and humidity are varied.

2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during maintenance and repair.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000261

2.7-E – Ability to support transport and storage physical environment conditions – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating stresses that occur during transport between storage locations and polling places.

2.7-F – Ability to support storage temperatures in physical environment – non-operating

The voting system must be able to withstand non-operating physical environmental conditions simulating temperature-related and humidity-related stresses that occur during storage.

2.7-G – Electrical disturbances

The voting system must continue to operate in the presence of electrical disturbances generated by other devices and people and must not cause electrical disruption to other devices and people.

Discussion

Voting devices located in a polling place or other places need to continue to operate despite disruption from electrical emanations generated by other devices, including static discharges from people. Likewise, voting devices need to operate without causing disruption to other devices and people due to electrical emanations from the devices.

2.7-H – Power outages, sags, and swells

The voting system must be able to withstand, without disruption of normal operation or loss of data, a complete loss of power lasting two hours.

Discussion

Essentially, battery backup must keep the voting system operational so that voting can continue for a minimum of two hours.

2.7-I – Withstand conducted electrical disturbances

All electronic voting systems must withstand conducted electrical disturbances that affect the power ports of the system.

AMERICAN OVERSIGHT

2.7-J – Emissions from other connected equipment

All elements of an electronic voting system must be able to withstand the conducted emissions generated by other elements of the voting system.

2.7-K – Electrostatic discharge immunity

All electronic voting systems must withstand, without disruption of normal operation or loss of data, electrostatic discharges (ESD) associated with human contact and contact with mobile equipment (such as service carts and wheelchairs).

Discussion

ESD events can originate from direct contact between an "intruder" (person or object) charged at a potential different from that of the units of the voting system, or from an approaching person about to touch the equipment – an "air discharge." The resulting discharge current can induce disturbances in the circuits of the equipment. This requirement is meant to ensure that voting devices are conformant to the typical ESD specifications met by other electronic devices used by the public such as ATMs and vending kiosks.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000263

Principle 3
Transparent

The voting system and voting processes are designed to provide transparency.

3.1 - The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.2 - The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000264

Principle 3
TRANSPARENT

The voting system and voting processes are designed to provide transparency.

Guideline 3.1 contains requirements for the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, and "system" refers to a voting system or individual voting device. The user documentation is also included in the technical date package (TDP) given to test labs. The sections in *3.1* cover

1 - System overview documentation covers documentation that explains the physical and logical structure of the system, its components, how it is structured, details about the software, and so forth.

2 - System performance documentation gives details on how the system performs in normal operation as well as its constraints and limits.

3 - System security documentation describes the features of the system that provide or contribute to its security and includes how to operate the system securely. Physical security and audit are included in this documentation.

4 - Software installation documentation describes in exact detail what software is installed, how it is installed, and how it is to be maintained.

5 - System operations documentation deals with operating and using the equipment to conduct elections, including setup, testing, voting operations, reporting, and so forth.

6 - System maintenance documentation deals with proper maintenance of the voting equipment and how to correct various issues or problems.

7 - Training material documentation lists what the manufacturer needs to cover about the personnel resources and training required for a jurisdiction to operate and maintain the system.

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation.

In 3.2, Setup inspection documentation explains how to verify that the system is properly setup and configured, and how to monitor its operations.

In 3.3, Public documentation requirements cover details of how a manufacturer codes the election event log, implements a CDF, builds barcodes, and implements audits.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000265

3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.1.1 – System overview documentation

3.1.1-A – System overview documentation

The manufacturer must provide system overview documentation that identifies the functional and physical components of the system, how the components are structured, and the interfaces between them.

3.1.1-B – System overview, functional diagram

System overview documentation must include high-level functional diagrams of the voting system that include all of its components. The diagrams must portray how the various components relate and interact.

Discussion

The diagrams could be engineering renderings or photographs.

3.1.1-C – System description

System overview documentation must include written descriptions and diagrams that present the following, as applicable:

1. a description of the functional components (or subsystems) as defined by the manufacturer (for example, environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships);
2. a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure;
3. a concept of operations that explains each system function and how the function is achieved in the design;
4. descriptions of the functional and physical interfaces between components;
5. identification of all COTS products (both hardware and software) included in the system or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component;
6. communications (dial-up, network) software;

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000266

7. interfaces among internal components and interfaces with external systems;
8. for components that interface with other components for which multiple products may be used, file specifications, data objects, or other means used for information exchange including the public standard used for such file specifications, data objects, or other means; and
9. benchmark directory listings for all software, firmware, and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.

Discussion

The diagrams could be engineering renderings or photographs.

3.1.1-D – Identify software and firmware by origin

System overview documentation must include full identification of all software and firmware items, indicating items that were:

1. written in-house including subcontracted;
2. procured as COTS, unmodified; and
3. procured as COTS and modified, including descriptions of the modifications to the software or firmware and to the default configuration options.

Description

Full identification would include authorship, version numbers, where procured, and other items to positively identify the COTs or in-house developed software

3.1.1-E – Traceability of procured software

System overview documentation must include a declaration that procured software items were obtained directly from the manufacturer or a licensed dealer or distributor.

Discussion

For most noncommercial software, this would mean a declaration that the software was downloaded from the canonical site or a trustworthy mirror. It is generally accepted practice for the core contributors to major open-source software packages to digitally sign the distributions. Verifying these signatures provides greater assurance that the package has not been modified.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000267

3.1.2 – System performance documentation

3.1.2-A – System performance documentation

The manufacturer must provide system performance documentation that includes:

1. device capacities and limits that were stated in the implementation statement;
2. if not already covered in the implementation statement, performance characteristics of each operating mode and function in terms of expected and maximum speed, throughput capacity, maximum volume (maximum number of voting positions and maximum number of ballot styles supported), and processing frequency;
3. quality attributes such as reliability, maintainability, availability, usability, and portability;
4. provisions for safety, security, privacy, and continuity of operation; and
5. design constraints, applicable standards, and compatibility requirements.

3.1.2-B – Maximum tabulation rate

System performance documentation must include the maximum tabulation rate for a bulk-fed scanner. This documentation must include the maximum tabulation rate for individual components that impact the overall maximum tabulation rate.

Discussion

The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems.

3.1.2-C – Reliably detectable marks

System performance documentation must include, for all types of optical scanners:

1. what constitutes a mark that is tabulatable;
2. what constitutes a mark that is ambiguous and may require adjudication; and
3. what constitutes a marginal mark that would not be tabulatable.

Discussion

Marginal marks could include those marks considered as stray or caused by defects or folds on the ballot.

AMERICAN OVERSIGHT

3.1.2-D – Processing capabilities

System performance documentation must include a listing of the system's functional processing capabilities, encompassing capabilities required by the VVSG, and any additional capabilities provided by the system, with a description of each capability. Therefore, this documentation must include the following attributes:

1. an explanation regarding the capabilities of the system that were declared in the implementation statement;
2. additional capabilities (extensions) must be clearly indicated;
3. required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated;
4. additional capabilities that function only when activated during installation or operation by the user must be clearly indicated; and
5. additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated.

3.1.3 – System security documentation

3.1.3-A – System security documentation

Manufacturers must provide a specific system security document that includes detailed information on the security architecture of the voting system and its security-related functions and how users are to properly employ them.

Discussion

This document is intended to further ensure transparency of the voting system. It includes a complete specification of the voting system security architecture, its different components, and how they work together when used properly. Information about security-related functions and components may also appear in other parts of the TDP as applicable but should also appear in this document. The document may contain detailed technical information but also is to contain usage instructions for employing security controls that are written clearly for the intended types of users, e.g., administrator, pollworker, etc.

3.1.3-B – Access control implementation

The system security document must include:

1. guidelines and usage instructions on implementing, configuring, and managing access control capabilities;

AMERICAN OVERSIGHT

2. an access control policy template or instructions to facilitate the implementation of the access control policy and associated access controls on the voting system;
3. an access control policy under which the voting system was designed to operate and a description of the hazards of deviating from this policy; and
4. information on all privileged accounts included on the voting system.

Discussion

Access control policy requirements include the minimum baseline policy definitions necessary for testing and implementing the voting system. The policies may be defined within the voting system or provided as guidelines in the documentation. The access control policy includes the assumptions that were made when the system was designed, the justification for the policy, and the hazards of deviating from the policy. Information on privileged accounts include the name of the account, purpose, capabilities, and permissions, and how to disable the account in the user documentation.

3.1.3-C – Physical security

The system security document must include an explanation of how to implement all physical security controls for voting devices and other security-sensitive components of the voting system, including model procedures necessary for effective use of countermeasures.

3.1.3-D – Audit procedures

The system security document must include an explanation of how to conduct audit procedures to determine whether tabulation is accurate.

3.1.4 – Software installation documentation

3.1.4-A – Software installation documentation

The manufacturer must provide software installation documentation that lists all software to be installed on the programmed devices of the voting system and the installation software used to install the software in the user documentation.

Discussion

Software to be installed on programmed devices of the voting system includes executable code, configuration files, data files, and election specific software.

AMERICAN OVERSIGHT

3.1.4-B – Software information

Software installation documentation must include the following information for each piece of software to be installed or used to install software on programmed devices of the voting system:

1. software product name;
2. software version number
3. software manufacturer name;
4. software manufacturer contact information;
5. type of software (application logic, border logic, third party logic, COTS software, or installation software);
6. list of software documentation; and
7. component identifiers (such as filenames) of the software, and type of software component (executable code, source code, or data).
8. flag to indicate whether or not the given software product should be considered "election-specific" (e.g., election-specific=[True|False]) to differentiate software used for implementing essential election application logic functions (such as counting) from more generic software (such as generic file-system functions).

3.1.4-C – Software location information

Software installation documentation must include the location (such as full path name or memory address) and storage device (such as type and part number of storage device) where each piece of voting system software is installed on programmed devices of the voting system.

Discussion

This requirement applies to voting system software installed on programmed devices of the voting system. The full directory path is the final destination of the software when installed on non-volatile storage with a file system.

3.1.4-D – Election specific software identification

Software installation documentation must identify election specific software in the user documentation.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000271

This requirement applies to voting system software installed on programmed devices of the voting system. If the documentation can provide information (such as what is indicated in item 8 from *3.1.4-B – Software information*) then this should be sufficient to clearly distinguish those pieces of software that perform essential election functions (such as counting) from those that perform more generic, non-election-specific tasks (such as those that might perform only general file-system operations, regardless of election concerns).

3.1.4-E – Installation software and hardware

Software installation documentation must include a list of software and hardware required to install software on programmed devices of the voting system in the user documentation.

3.1.4-F – Software installation procedures

Software installation documentation must include the software installation procedures used to install software on programmed devices of the voting system in user documentation.

3.1.4-G – Baseline image creation

To replicate programmed device configurations, the software installation procedures must create a baseline image of the initial programmed device configuration with storage media and mechanism for verifying the image's validity using a digital signature.

3.1.4-H – Programmed device configuration replication

The software installation procedures must use the baseline image and associated digital signature and digital signature validation mechanism of the initial validated image to replicate the configuration onto other programmed devices.

Discussion

The main point of this requirement is to ensure transitive immutability of a given device configuration (based on a valid, original image that corresponds to an original cryptographic signature). In this way, it seeks to ensure that the starting image that is used for the replication of an image to a particular configuration or target device is the same as the one that was validated via digital signature mechanisms.

The process for dealing with varying details of alternative target platforms can be addressed with the use of modern deployment technologies to create configurable installation mechanisms. This is not uncommon for major software technology providers. Thus, technology providers will be expected to develop appropriate install and configuration mechanisms that can have configurable images that can be signed through this digital signature mechanism at the outset and when replicating to any

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000272

target configuration to ensure that both the image and the mechanisms for transforming that image in a given target deployment environment have been understood and validated from the beginning.

The above descriptions are meant to provide a way to validate a much wider range of deployment scenarios than has been experienced in the past. As a result, it is not expected or intended that this process would necessarily require strictly binary images, but rather, configurable ones, with the configuration settings and mechanisms for installation and signature verification provided, signed, and validated from the beginning.

3.1.4-I – Software installation record creation

The software installation procedures must specify the creation of a software installation record that includes at a minimum:

1. a unique identifier (such as a serial number) for the record;
2. a list of unique identifiers of storage media associated with the record;
3. the time, date, and location of the software installation;
4. names, affiliations, and signatures of all people present;
5. copies of the procedures used to install the software on the programmed devices of the voting system;
6. the certification number of the voting system;
7. list of the software installed as well as associated digital signatures and mechanisms for installation and verification on programmed devices of the voting system; and
8. a unique identifier (such as a serial number) of the vote-capture device or election management system (EMS) which the software is installed.

Discussion

The purpose of this requirement is a continuation of *3.1.4-I – Software installation record creation*, to ensure transitive immutability from the original baseline image through a given installation process (i.e., installation of certified software).

The requirement emphasizes the importance of the final act of performing an installation of certified software on a target system configuration. It is a requirement to ensure that this event have some means by which an appropriate record, attesting to the facts of the installation event itself, can be produced and can provide the given information.

Creators of software installation mechanisms and procedures are asked to provide information in their installation user documentation specifying the elements of this record and that it should be recorded in the event of a certified software installation.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000273

Related requirements: 3.1.4-H – Programmed device configuration replication

3.1.4-J – Procurement of voting system software

Software installation documentation must include that voting system software be obtained from a trusted distribution repository.

Discussion

Distribution repositories provide software they receive to parties approved by the owner of the software.

3.1.4-K – Open market procurement of COTS software

Software installation documentation must include that COTS software be obtained from the open market.

3.1.4-L – Erasable storage media preparation

Software installation documentation must specify how previously stored information on erasable storage media is removed before installing software on the media.

Discussion

The purpose of this requirement is to prepare erasable storage media for use by the programmed devices of the voting system. The requirement does not mandate the prevention of previously stored information leakage or recovery. Simply deleting files from file systems, flashing memory cards, and removing electrical power from volatile memory satisfies this requirement.

3.1.4-M – Trusted storage media

Software installation documentation must specify that trusted storage media be used to install software on programmed devices of the voting system.

Discussion

Trusted storage media can include read-only media.

Previous VVSGs emphasized the use of unalterable storage media which is believed to be too restrictive in the current technological context. Instead, it is preferable that read-only storage be used. And, as indicated in related requirements, it is assumed that any use of media, transport, or use of original images be associated with a mechanism for verifying the cryptographic signatures of those original images.

Related requirements: 3.1.4-H – Programmed device configuration replication
3.1.4-I – Software installation record creation

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000274

3.1.5 – System operations documentation

3.1.5-A – System operations documentation

Manufacturers must provide a specific system operations document for use by all personnel who support pre-election and election preparation, polling place activities, and central counting activities, as applicable, with regard to all system functions and operations. It must:

1. provide a detailed description of procedures required to initiate, control, and verify proper system operation;
2. provide procedures that clearly enable the operator to assess the correct flow of system functions (as evidenced by system-generated status and information messages);
3. provide procedures that clearly enable the administrator to intervene in system operations to recover from an abnormal system state;
4. define and illustrate the procedures and system prompts for situations where operator intervention is required to load, initialize, and start the system;
5. define and illustrate procedures to enable and control the external interface to the system operating environment if supporting hardware and software are involved. (This information is provided for the interaction of the system with other data processing systems or data interchange protocols.);
6. provide administrative procedures and off-line operator duties (if any) if they relate to the initiation or termination of system operations, to the assessment of system status, or to the development of an audit trail;
7. support successful election definition and software installation and control by central election officials;
8. provide a schedule and steps for the software and ballot installation, including a table outlining the key dates relative to the start of voting, events, and deliverables; and
9. specify diagnostic tests that may be employed to identify problems in the system, verify the correction of problems, and isolate and diagnose faults from various system states.

Discussion

The nature of the instructions for operating personnel will depend upon the overall system design and required skill level of system operations support personnel.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000275

3.1.5-B – Support training

The operations document must include all information that is required for the preparation of detailed system operating procedures and for the training of administrators, central election officials, election judges, and election workers.

3.1.5-C – Functions and modes

The operations document must include a summary of system operating functions and modes to permit understanding of the system's capabilities and constraints.

3.1.5-D – Roles

The operations document must identify the roles of operating personnel and relate them to the operating modes of the system.

3.1.5-E – Conditional actions

The operations document must describe decision criteria and conditional operator functions such as error and failure recovery actions.

3.1.5-F – References

The operations document must list all reference and supporting documents pertaining to the use of the system during election operations.

3.1.5-G – Operational environment

The operations document must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment operations, including a statement of all requirements and restrictions regarding:

1. environmental protection;
2. electrical service;
3. recommended auxiliary power;
4. telecommunications service; and
5. any other facility or resource required for the proper installation and operation of the system.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000276

3.1.5-H – Readiness testing

The operations document must include specifications for testing system installation and readiness.

Discussion

Readiness testing refers to steps that election officials can take after configuring equipment to establish that it was correctly configured. Logic and accuracy testing would be part of this.

3.1.5-I – Features

The operations document must include documentation of system operating features that includes:

1. detailed descriptions of all input, output, control, and display features accessible to the operator or voter;
2. examples of simulated interactions to facilitate understanding of the system and its capabilities;
3. sample data formats and output reports; and
4. illustration and description of all status indicators and information messages.

3.1.5-J – Support

The operations document must include documentation of system operating procedures that:

1. describes procedures for providing technical support, system maintenance, and correction of defects, and for incorporating hardware upgrades and new software releases; and
2. defines the procedures required to support system installation and readiness testing.

3.1.5-K – Transportation and storage

The operations document must include any special instructions for the care and handling of voting devices and any removable media or records for:

1. shipment;
2. storage; and
3. archiving information.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000277

3.1.6 – System maintenance documentation

3.1.6-A – System maintenance documentation

Manufacturers must include system maintenance documentation that provides information to support election workers, information systems personnel, or maintenance personnel in adjusting or removing and replacing components or modules in the field.

Discussion

Election workers such as polling place workers may not be permitted to replace components, however in some cases they may be permitted to adjust them. Thus, the documentation should be geared to the appropriate personnel.

3.1.6-B – General contents

Maintenance documentation must include service actions recommended to correct malfunctions or problems, personnel and expertise required to repair and maintain the system, and equipment and materials facilities needed for proper maintenance.

3.1.6-C – Maintenance viewpoint

Maintenance documentation must include the structure and function of the hardware, firmware, and software for election preparation, programming, vote recording, tabulation, and reporting in sufficient detail to provide an overview of the system for maintaining and identifying faulty hardware or software.

3.1.6-D – Equipment overview details

Maintenance documentation must include a concept of operations that fully describes such items as:

1. electrical and mechanical functions of the equipment;
2. for paper-based systems, how ballot handling and reading processes are performed;
3. for electronic vote-capture devices, how vote selection and ballot casting are performed;
4. how data transmission over a network is performed (if applicable);
5. how data are handled in memory units;
6. how data output is initiated and controlled;
7. how power is converted or conditioned; and

AMERICAN OVERSIGHT

8. how test and diagnostic information is acquired and used.

Discussion

The documentation should indicate how and when information is written from volatile to non-volatile memory, including redundant storage.

3.1.6-E – Maintenance procedures

Maintenance documentation must include preventive and corrective maintenance procedures for hardware, firmware, and software.

3.1.6-F – Preventive maintenance procedures

Maintenance documentation must identify and describe:

1. all required and recommended preventive maintenance tasks, including software and data backup, database performance analysis, and database tuning;
2. the number and skill levels of personnel required for each task;
3. the parts, supplies, special maintenance equipment, software tools, or other resources needed for maintenance; and
4. any maintenance tasks that must be coordinated with the manufacturer or a third party (such as coordination that may be needed for COTS used in the system).

3.1.6-G – Troubleshooting procedure details

Maintenance documentation must identify specific procedures to be used in diagnosing and correcting problems in the system hardware, firmware, and software. Descriptions must include:

1. steps to replace failed or deficient equipment;
2. steps to correct deficiencies or faulty operations in software or firmware;
3. modifications that are necessary to coordinate any modified or upgraded software or firmware with other modules;
4. number and skill levels of personnel needed to accomplish each procedure;
5. special maintenance equipment, parts, supplies, or other resources needed to accomplish each procedure; and
6. any coordination required with the manufacturer, or other party, for COTS.

AMERICAN OVERSIGHT

3.1.6-H – Special equipment

Maintenance documentation must identify and describe any special purpose test or maintenance equipment recommended for fault isolation and diagnostic purposes.

3.1.6-I – Parts and materials

Maintenance documentation must include detailed documentation of parts and materials needed to operate and maintain the system.

3.1.6-J – Approved parts list

Maintenance documentation must include a complete list of approved parts and materials needed to operate and maintain the system. This list must contain sufficient descriptive information to identify all parts by:

1. type,
2. size,
3. value or range,
4. manufacturer's designation,
5. individual quantities needed, and
6. sources from which they may be obtained.

3.1.6-K – Marking devices

Maintenance documentation must identify specific marking devices that, if used to make the prescribed form of mark, produce readable marked ballots so that the system meets the performance requirements for accuracy.

Discussion

Includes pens or pencils and possibly a compatible ballot marking device (BMD).

3.1.6-L – Approved manufacturers

Maintenance documentation must include a listing of sources and model numbers for marking devices manufactured by multiple external sources that satisfy these requirements.

3.1.6-M – Ballot stock specification

Maintenance documentation must:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000280

1. specify the required paper stock, weight, size, shape, opacity, color, watermarks, field layout, orientation, size and style of printing, size, and location of vote response fields; and
2. identify unique ballot styles, placement of alignment marks, ink for printing, and folding and bleed-through limitations for preparation of ballots that are compatible with the system.

3.1.6-N – Ballot stock specification criteria

Maintenance documentation for optical scanners must include specifications for ballot materials to ensure that votes are read from only a single ballot at a time, without bleed-through or transferal of marks from one ballot to another.

3.1.6-O – Printer paper specification

Maintenance documentation for voting systems that include printers must include specifications of the paper necessary to ensure correct operation and minimize jamming.

Discussion

This requirement covers all printers, either stand-alone or integrated with another device, regardless whether they are used for reporting, for logging, for voter verified paper records (VVPR), etc.

3.1.6-P – System maintenance, maintenance environment

Maintenance documentation must identify all facilities, furnishings, fixtures, and utilities that will be required for equipment maintenance.

3.1.6-Q – System maintenance, maintenance support and spares

Maintenance documentation must identify:

1. recommended number and locations of spare devices or components to be kept on hand for repair purposes during periods of system operation;
2. recommended number and locations of qualified maintenance personnel who need to be available to support repair calls during system operation; and
3. organizational affiliation (for example, jurisdiction, manufacturer) of qualified maintenance personnel.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000281

3.1.7 – Training documentation

3.1.7-A – Training documentation

The manufacturer must describe the personnel resources and training required for a jurisdiction to operate and maintain the system.

3.1.7-B – Personnel

The manufacturer must specify the number of personnel and skill levels required to perform each of the following functions:

1. pre-election or election preparation functions (such as, entering an election, contest and candidate information, designing a ballot, and generating pre-election reports);
2. system operations for voting system functions performed at the polling place;
3. system operations for voting system functions performed at the central count facility;
4. preventive maintenance tasks;
5. diagnosis of faulty hardware, firmware, or software;
6. corrective maintenance tasks; and
7. testing to verify the correction of problems.

3.1.7-C – User functions versus manufacturer functions

The manufacturer must distinguish which functions may be carried out by user personnel and which must be performed by manufacturer personnel.

3.1.7-D – Training requirements

The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, and election workers.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000282

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.2-A – Setup inspection process

Manufacturers must provide setup inspection process documentation that includes the setup inspection process that the voting device was designed to support including a description of the risks of deviating from the process.

Discussion

The setup inspection process provides a means to inspect various properties of voting devices as needed during the election process.

3.2-B – Minimum properties included in the setup inspection process

Setup inspection process documentation must at a minimum include:

1. inspecting voting system software;
2. inspecting storage locations that hold election information that changes during an election;
3. inspecting other voting device properties; and
4. executing logic and accuracy testing related to readiness of use in an election.

3.2-C – Setup inspection record generation

Setup inspection process documentation must describe the records that result from performing the setup inspection process.

3.2-D – Installed software identification procedure

Setup inspection process documentation must include the procedures to identify all software installed on programmed devices of the voting system.

Discussion

This requirement provides the ability to identify if the proper software is installed and that no other software is present on programmed devices of the voting system. This requirement covers software stored on storage media with or without a file system.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000283

3.2-E – Software integrity verification procedure

Setup inspection process documentation must include the procedures to verify the integrity of software installed on programmed devices of the voting system.

3.2-F – Election information value

Setup inspection process documentation must include a list of voting device storage locations for holding election information that can change during the election, except for the static values set to conduct a specific election.

3.2-G – Maximum and minimum values of election information storage locations

Setup inspection process documentation must include the maximum and minimum values of voting device storage locations for holding election information that can change during an election.

3.2-H – Variable value inspection procedure

Setup inspection process documentation must include the procedures to inspect the values of voting device storage locations for holding election information that can change during an election.

3.2-I – Backup power operational range

Setup inspection process documentation must include the nominal operational range for the backup power sources of the voting device.

3.2-J – Backup power inspection procedure

Setup inspection process documentation must include the procedures to inspect the remaining charge of the backup power sources of the voting device.

3.2-K – Cabling connectivity inspection procedure

Setup inspection process documentation must include the procedures to inspect the connectivity of the cabling attached to the voting device.

3.2-L – Communications operational status inspection procedure

Setup inspection process documentation must include the procedures to inspect the operational status of the communications capabilities of the voting device.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000284

3.2-M – Communications on/off status inspection procedure

Setup inspection process documentation must include the procedures to inspect the on/off status of the communications capabilities of the voting device.

3.2-N – Quantity of voting equipment

Setup inspection process documentation must include a list of consumables associated with the voting device, including estimated number of usages per unit.

3.2-O – Consumable inspection procedure

Setup inspection process documentation must include the procedures to inspect the remaining amount of each of the voting device's consumables.

3.2-P – Calibration of voting device components

Setup inspection process documentation must include:

1. a list of components associated with the voting device that require calibration;
2. the nominal operating ranges for each component;
3. the procedures to inspect the calibration of each component; and
4. the procedures to adjust the calibration of each component.

3.2-Q – Checklist of properties to be inspected

Setup inspection process documentation must include a checklist of other properties of the voting device to be inspected, to include:

1. a description of the risks of not performing each documented inspection;
2. power sources;
3. cabling for communications;
4. capabilities;
5. consumables;
6. calibration of voting device components;
7. general physical features of the voting device; and
8. securing external interfaces of the voting device not being used.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000285

3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.

3.3-A – System security, system event logging

Manufacturers must provide publicly available documentation that:

1. describes system event logging capabilities and usage, and
2. fully documents the log format information.

Discussion

The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent manufacturers to implement utilities to parse the log file. This documentation must be publicly available and not just in the TDP.

3.3-B – Specification of common data format usage

Manufacturers must provide publicly available documentation describing how the manufacturer has implemented a CDF specification for a particular device or function. This includes such items as:

1. descriptions of how elements and attributes are used;
2. constraints on data elements; and
3. extensions as well as any constraints.

Discussion

Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a CDF specification for its voting devices and the types of data exchanged or exported. Here is list of related references: *NIST SP 1500-103 Cast Vote Records Common Data Format Specification [CVR_CDF], NIST SP 1500-100 Election Results Common Data Format Specification [NIST16], NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF], NIST SP 1500-102 Voter Records Interchange(VRI) CDF Specification [VRI_CDF].*

3.3-C – Bar and other codes

Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material.

Discussion

AMERICAN OVERSIGHT

The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to develop applications that examine the barcoded contents.

3.3-D – Ballot selection codes

The voting system must be capable of producing a report on an election-by-election basis to show the meaning of codes and other data used within barcodes and CVRs to represent ballot selections and ballot style information.

Discussion

Codes that represent a voter's ballot selections are commonly used within barcodes and CVRs so as to save space. The codes will likely change for each election. The codes are meaningless to a voter or an auditor unless the voting system can produce a report that shows all codes possible and what contests and ballot selections they represent. If, for example, a code of 90 is used to represent a particular contest, then the report must show that 90 refers to the title or description of that particular contest. This includes other information within the barcode generally found on clear-text ballots to identify the ballot style.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000287

Principle 4
Interoperable

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 - Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.2 - Standard, publicly available formats for other types of data are used, where available.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet applicable VVSG requirements.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000288

Principle 4
INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

This principle covers requirements that ensure all system data is in an interoperable format and explains when standard, publicly available formats are used. It also addresses widely used hardware interfaces and when COTS devices are permitted. The guidelines under *Principle 4* are:

1 - Interoperable formats requirements, which include voting system data that is imported, exported, or otherwise reported.

2 - Standard formats covering when publicly available formats for other types of data not addressed by CDF specifications can be used.

3 - Interfaces and communication protocols, describing the need to use standard hardware interfaces and communication protocol when connecting devices.

4 - COTS covering the requirement that any COTs devices used meet all applicable requirements.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000289

4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.1-A – Election programming data input and output

The voting system must include support for CDF specification(s) regarding:

1. import and export of election programming data, and
2. import and export of ballot programming data.

Discussion

This requirement concerns import and export of pre-election data into an election definition device, such as for identification of political geography, contest, candidate, ballot data, and other pre-election information used to setup an election and produce ballots. This also includes reports of pre-election data from the election definition device that can be used to verify the election programming setup. More information can be found in *SP 1500-100 Election Results Common Data Format Specification [NIST16].*

4.1-B – Tabulator report data

The voting system must include support for CDF specification(s) for import and export of election results reporting data.

Discussion

Importing results data is required to provide support for aggregations of vote data from different election management systems such as what occurs during state roll-ups on election night and during the process of election results certification. More information can be found in: NIST SP 1500-100 *Election Results Common Data Format Specification [NIST16]*.

4.1-C – Exchange of cast vote records (CVRs)

The voting system's audit, casting, tabulation, and vote-capture functions dealing with CVRs must have the capability of importing or exporting CVRs according to CDF specification(s).

Discussion

Devices that export or import CVRs typically include voter-facing and batch-fed scanners, election management systems, and other devices used for adjudication or auditing. This requirement indicates that these devices have the capability to import or export CVRs in the respective CDF(s). More information can be found in: NIST SP 1500-103 *Cast Vote Records Common Data Format Specification [CVR_CDF].*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000290

4.1-D – Exchange of voting device election event logs

The voting devices comprising the voting system must include support for CDF specification(s) for import or export of election event log data.

Discussion

This requirement refers to election event logs and not system logs provided by common operating systems such as Microsoft Windows or Apple iOS. This requirement does not mandate that manufacturers use the format for storing election log information; a manufacturer can meet this requirement by conversion or translation from a native format into the CDF. More information can be found in:], *NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF].*

4.1-E – Voting device event code documentation

Manufacturers must provide a publicly available specification for event codes used in their equipment.

Discussion

Use of *NIST SP 1500-101 Election Event Logging Common Data Format Specification [LOG_CDF]* for election event logs only addresses the data format; it does not mandate a common lexicon for event codes. *NIST SP 1500-101 [LOG_CDF]* provides a separate schema for including documentation of event codes; manufactures may make this available publicly or upon request without condition.

4.1-F – Specification of common format usage

Manufacturers must include a specification describing how the manufacturer has implemented a CDF specification for a particular device or function. This includes such items as descriptions of how elements and attributes are used, as well as any constraints or extensions.

Discussion

Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a CDF specification for its voting devices and the types of data exchanged or exported.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000291

4.2 - Standard, publicly available formats for other types of data not addressed by CDF specifications are used.

4.2-A – Standard formats

Publicly available non-proprietary formats must be used, where possible, for exchanging data.

Discussion

Examples include the use of common data encodings such as bar or QR codes.

4.2-B – Public documented manufacturer formats

Where publicly available non-proprietary formats are not available, manufacturers must include a specification that describes the protocol or data format.

Discussion

As an example, a manufacturer's algorithm or method for packing or compressing data before encoding in a QR code will be documented so that its implementation and usage is available publicly.

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.3 – Interfaces and communication protocols

4.3-A – Standard device interfaces

Standard, common hardware interfaces and protocols must be used to connect devices.

Discussion

Examples include using published communications protocols, such as, IEEE, and using common hardware interfaces, such as, USB, when connecting to printers, disks, and other devices.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000292

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet all applicable VVSG requirements.

4.4-A – COTS devices meet applicable requirements

COTS devices, if used, must satisfy all applicable VVSG requirements.

Discussion

As an example, use of a COTS scanner to scan ballots is potentially possible, but it will need to meet applicable environmental and electrical requirements and, potentially, other requirements depending on how the scanner is used. For example, if it is used to create CVRs, it will need to meet those requirements dealing with CVR creation and handling.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000293

Principle 5
Equivalent and Consistent Voter Access

All voters can access and use the voting system regardless of their abilities.

5.1 - Voters have a consistent experience throughout the voting process within any method of voting.

5.2 - Voters receive equivalent information and options in all modes of voting.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000294

Principle 5
EQUIVALENT AND CONSISTENT VOTER ACCESS

All voters can access and use the voting system regardless of their abilities.

Principle 5 ensures that all voters can cast their votes easily and accurately, regardless of any disabilities they may have. This fulfills the requirements of the *Help America Vote Act (HAVA), Section 301(a)(3) [HAVA02]* which states, "The voting system shall (A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."

It also addresses *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]* which requires that electronic and information technology be accessible to people with disabilities, and the language access requirements in the *Voting Rights Act (VRA) [VRA65]*.

The goal of both guidelines in *Principle 5* is to ensure that everyone can use the voting system, regardless of their abilities or preferences. Voting equipment can present ballot choices in a variety of ways which make it possible for people with a wide range of disabilities to vote. The equipment must also fully support all the languages that the manufacture claims to support. The big differences are that guidelines:

1 – Consistent experience also covers the requirement that all vote records must be auditable by those who speak only English. Also, in addition to actually casting their votes, voters must have access to those same display formats and interaction modes for all information and instructions related to casting those votes.

2 – Equivalent information also addresses the requirement that these display formats (visual, audio, enhanced visual) and interaction modes (touch, tactile, limited dexterity) must offer consistent and equivalent support for the actions required to vote, and offer them in a way that does not introduce bias. In addition, if the voter switches formats mid-stream, for example from visual to audio or from Spanish to English, the system must preserve all settings and votes cast.

Finally, note that this principle's requirements, including supporting the display formats and interaction modes listed in *5.1-A – Voting methods and interaction modes*, also apply to all of the usability and accessibility requirements in *Principles 6-8*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000295

5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1-A – Voting methods and interaction modes

Within any method of voting, all display formats including enhanced visual and audio and all interaction modes including tactile and limited dexterity must have the same functionality as the visual format and touch mode including voting, verification, and casting.

Discussion

Methods of voting that a voting system might support include in-person voting, vote-by-mail, remote ballot marking, among others. The VVSG scope is in-person voting. For voting systems to meet this requirement they would need to include, for example:

- Features that support limited dexterity interaction to enable voters who lack fine motor control or the use of their hands, to submit their ballots privately and independently without manually handling the ballot.
- Features for paper ballots or paper verification records that assist voters with poor reading vision to read these ballots and records.
- Features to allow blind voters and voters with limited dexterity to perform paper-based verification or feed their own optical scan ballots into a scanner, if all other voters do so. For example, ballot papers or smart cards might provide tactile cues that allow the correct insertion of the card.
- Support for all voting variations. For example, if a visual ballot supports voting a straight-party ticket and then changing the vote for a single contest, so do all other display formats and interaction modes.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

5.1-B – Languages

The voting system must be capable of displaying and printing the ballot, contest options, review screens, voter verifiable paper records, and voting instructions in all languages the manufacturer has declared the system supports, in both visual and audio formats where applicable.

Discussion

Both written and unwritten languages are within the scope of this requirement.

The system will be tested in all languages that the manufacturer claims it is capable of supporting.

This requirement originates with the *VRA [VRA65]*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000296

5.1-C – Vote records

All records, including paper ballots and voter verifiable paper records, must have the information required to support auditing by election workers and others who can only read English.

Discussion

Although the system needs to be easily usable by voters using an alternative language, records of the vote also need to be fully available to English-only readers to support election administration and auditing. See *9.4 - The voting system supports efficient audits* for related requirements.

To meet this requirement, a paper ballot may not be a fully bilingual ballot. For instance, the full text of a ballot question might appear only in the alternative language, but the contest option (for example, “yes / no”) needs to be readable by English-only readers.

5.1-D – Accessibility features

Accessibility features must be integrated into the manufacturer’s voting system so accessibility for voters with disabilities is supported throughout the voting session, including any steps to activate the ballot at the voting station, ballot marking, verification, and casting.

Discussion

This requirement ensures accessibility to the voter throughout the entire session. Not only are individual system components (such as ballot markers, paper records, and optical scanners) accessible, but they also support voters with disabilities throughout the process of voting from activation through casting. Requirements for individual system components are described in *Principle 7: Marked, Verified, and Cast as Intended*. This general requirement supports *HAVA [HAVA02].*

Related requirements: 6.1-B – Warnings

5.1-E – Reading paper ballots

If the voting system generates a paper record (or some other durable, human-readable record) that can be the official ballot or determinative vote record, then the voting system must allow the voter to verify the paper record using the same access features they used to mark the ballot, including enhanced visual and audio formats and tactile and limited dexterity modes.

Discussion

Paper records present difficulties for voters who use large font, high contrast, alternative languages, and other settings. The purpose of this requirement is to ensure that all voters have a similar

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000297

opportunity for vote verification. For ballot marking devices, for example, if the voter is using audio to make their selections, the voter verifiable paper record, not the stored voter selections, must be read back.

This requirement allows the voter to use the same access features throughout the entire voting session. It also does not preclude the voter from choosing a different access feature to verify the record. For example, the voting system might provide a reader that converts the paper record contents into audio output.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.1-I – Text size (paper)

5.1-F – Accessibility documentation

As part of the overall system documentation the manufacturer must include descriptions and instructions for all accessibility features that describe:

- recommended procedures that fully implement accessibility for voters with disabilities, and
- how the voting system supports those procedures.

Discussion

The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Related requirements: 7.3-N – Instructions for voters
7.3-O – Instructions for election workers

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000298

5.2 – Voters receive equivalent information and options in all modes of voting.

5.2-A – No bias

The voting system must not introduce bias for or against any of the contest options presented to the voter. In enhanced visual and audio formats and tactile and limited dexterity modes, all ballot options are to be presented in an equivalent manner.

Discussion

Certain differences in ballot presentation are mandated by state law, such as the order in which candidates are listed and provisions for voting for write-in candidates. This requirement ensures that comparable characteristics such as font size or audio volume and speed are the same for all ballot options.

5.2-B – Presenting content in all languages

All information that is presented to the voter in English must also be capable of being presented in all other languages that are supported, whether the language is in visual or audio format. This includes instructions, warnings, messages, notification of undervotes or overvotes, contest options, and vote verification information.

Discussion

It is not sufficient simply to present the ballot options in the alternative languages. All the supporting information voters need to mark their ballot is also covered in this requirement.

This requirement originates with the *VRA [VRA65]*.

5.2-C – Information in all modes

Instructions, warnings, messages, notifications of undervotes or overvotes, and contest options must be presented to voters in the display formats and interaction modes required in *5.1-A – Voting methods and interaction modes*. This includes voting, verification, and casting.

Discussion

For audio mode, this requirement can be met with an audio that includes cues to help users know what to expect. For example, announcing the number of items in a list of candidates or contests makes it easier to jump from one item to another without waiting for the audio to complete. Audio cues also ensure that the voter is aware of possible undervotes or overvotes. This includes information about activation.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000299

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

5.2-D – Audio synchronized

The voting system must provide the option for synchronized audio output to convey the same information that is displayed visually to the voter.

Discussion

This requirement covers all information, including information entered by the voter such as write-in votes.

This requirement applies to any audio output, whether it is recorded or generated as text-to-speech.

Any differences between audio and visual information are for functional purposes only, with variations only based on differences in the display format and interaction mode, especially for instructions.

This feature can assist voters with cognitive disabilities.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

5.2-E – Sound cues

Sound and visual cues must be coordinated so that:

- sound cues are accompanied by visual cues unless the system is set to audio-only; and
- visual cues are accompanied by sound cues unless the system is set to visual-only.

Discussion

The voting equipment might beep if the voter attempts to overvote. If so, there has to be an equivalent visual cue, such as the appearance of an icon or a blinking element. If the voting system has been set to audio-only, there would be no visual cue.

Audio output also supports non-written languages, voters with low literacy, or voters with low vision.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

5.2-F – Preserving votes

At any time during a voting session, an electronic voting interface must allow the voter to change all language and display format options, and the interaction settings that the voter can chose directly, while preserving all current vote selections. When changing settings, the

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000300

system must preserve navigation, screen position, visual settings, audio settings, and other information within and across contests.

Discussion

A voter who initially chooses an English version of the ballot might switch to another language in order to read a referendum question.

Many blind voters have preferences for audio settings, including the rate of speech and volume that are important for comprehension.

Changing visual settings for text size might change the layout of the information on the screen, making it important to maintain the screen position.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000301

Principle 6
Voter Privacy

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record, without assistance from others.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000302

Principle 6
VOTER PRIVACY

Voters can mark, verify, and cast their ballot privately and independently.

Privacy for voters refers to the property of a voting system that is designed and deployed to enable voters to obtain a ballot, and mark, verify, and cast it without revealing their ballot selections or selections of language, display formats, and interaction modes to anyone else.

Privacy covers:

- electronic and paper interfaces,
- audio and visual systems, and
- warning systems that must also preserve confidentiality.

Principle 6: Voter Privacy, covers voter privacy during voting. Requirements in *Principle 6* help ensure private and independent voting as mandated in the Help America Vote Act (HAVA).

The related *Principle 10: Ballot Secrecy* covers preventing links between a voter and a ballot after the ballot has been cast.

The guidelines under *Principle 6* cover:

1 – Privacy of interaction which describes the requirement that the voting process preserves the privacy of the voter's interaction with the ballot, display format and other options for voting, and vote selections.

2 – Voting without assistance which mandates that voters can mark, verify, and cast their ballot or other cast vote record without assistance from others.

AMERICAN OVERSIGHT

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.1-A – Preserving privacy for voters

Privacy for voters must be preserved during the entire voting session including ballot activation, voting, verifying, and casting the ballot.

Discussion

This requirement allows for different approaches for electronic and paper interfaces.
In both cases, appropriate shielding of the voting station is important -- for example, privacy screens for the voting stations.

When a paper record with ballot information needs to be transported by the voter, devices such as privacy sleeves can be necessary. This requirement applies to all records with information on votes (such as a vote verification record) even if that record is not itself a ballot.

This requirement supports *HAVA [HAVA02]*.

Related requirements: 7.2-F – Voter speech

6.1-B – Warnings

During the voting session, the voting system must issue all warnings in a way that preserves privacy for voters and the confidentiality of the ballot.

Discussion

HAVA 301 (a)(1)(C) [HAVA 02] mandates that the voting system notifies the voter of an attempted overvote in a way that preserves privacy for voters and the confidentiality of the ballot. This requirement addresses that mandate.

Related requirements: 7.3-K– Warnings, alerts, and instructions

6.1-C – Enabling or disabling output

During the voting session, the voting system must make it possible for the voter to independently enable or disable either the audio or the visual output and be notified of the change, resulting in a visual-only or audio-only presentation.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000304

Voters can be notified of the change to the display or audio output in a variety of ways including beep, voice, or visual notification. An unobtrusive notification that the system has changed the visual display format is helpful to voters who cannot see the screen to confirm the change visually.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 7.2-A – Display and interaction options
7.3-K – Warnings, alerts, and instructions

6.1-D – Audio privacy

Audio during the voting session must be audible only to the voter.

Discussion

Voters who are hard of hearing but need to use an audio interface sometimes need to increase the volume of the audio. Such situations require headphones or other devices (such as a hearing loop) with low sound leakage so the contents of the audio cannot be overheard and understood by others.

Voters who are hard of hearing can share audio interfaces with their designated assistants.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 7.2-F – Voter speech
8.1-J – Hearing aids

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000305

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record without assistance from others.

6.2-A - Voter independence

Voters must be able to mark, verify, and cast their ballot or other associated cast vote records independently and without assistance from others.

1. If a voting system includes any features voters might use after casting a ballot as part of end-to-end (E2E) verifiable system ballot tracking, they must be accessible.

Discussion

This requirement ensures that voters can vote with their own interaction preferences and without risk of intimidation or influence.

HAVA 301 (a)(1)(C)[HAVA02] mandates that the voting system be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters. This requirement directly addresses this mandate.

Note that in addition to features for voters after casting their ballot for E2E system ballot tracking, there are other features not in the scope of VVSG requirements that should be designed for accessibility such as forms or notices to cure problems with a vote-by-mail ballot, and sites to learn whether a provisional ballot was accepted for counting.

Related requirements:
- 2.2-A – User-centered design process
- 5.1-D – Accessibility features
- 5.1-E – Reading paper ballots
- 8.2-A – Federal standards for accessibility

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000306

Principle 7
Marked, Verified, and Cast as Intended

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 - The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.2 - Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes and selections.

7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000307

Principle 7
MARKED, VERIFIED, AND CAST AS INTENDED

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

This principle covers the core actions of voting, supporting voters in marking, verifying, and casting their ballot. It includes all voting systems including both paper ballots and electronic interfaces.

The requirements in *Principle 7* are derived from federal laws, including:

- the *Help America Vote Act of 2002 (HAVA)*,
- *Section 508* (part of the *Rehabilitation Act of 1973*)
- *Web Content and Accessibility Guidelines (WCAG)*, and,
- the *Voting Rights Act*.

This principle is divided into three sections which follow 508/ WCAG's well-known organizing principles of Perceivable, Operable, and Understandable. Robust, the final POUR principle is included in *Principle 8 – Robust, safe, usable and accessible*. The guidelines under *Principle 7* are:

1 – Default settings covers how ballot information is presented using audio and visual settings, as well as the voter's ability to adjust the voting system to meet their needs or preferences. This includes using color and contrast, adjusting font size, and ensuring audio settings result in understandable speech.

2 – Controls covers a voter's operation of the voting system, that is, the interaction with and control of the ballot during voting, including how the information is displayed and the voter's ability to navigate the system. It addresses the voter's ability to scroll though the electronic ballot, use the audio and touch controls, and use simple gestures. It also includes the need for adequate space for those who use wheelchairs. Both voters and election workers must be able to use all controls accurately.

3 – Understandable information covers the ability of the voter to understand all information on the ballot as it is presented, including instructions and messages from the system. Among other elements, it includes preventing contest layouts that can cause confusion, making clear the maximum number of choices a voter has, notifying the voter of any errors on the ballot (such as overvotes) before it is cast, and letting the voter know when they have successfully voted. It also covers ensuring that instructions for election workers are understandable.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000308

7.1 – The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.1-A – Reset to default settings

If the adjustable settings of the voter interface have been changed by the voter or election worker during the voting session, the system must automatically reset to the default setting when the voter finishes voting, verifying, and casting.

Discussion

This ensures that the voting system presents the same initial appearance to every voter.

This requirement covers all settings that can be adjusted, including font size, color, contrast, audio volume, rate of speech, turning on or off audio or video, and enabling alternative input devices.

Applies to:	Electronic interfaces
Related requirements:	7.1-K – Audio settings

7.1-B – Reset by voter

If either the voter or an election worker can adjust the settings of the voter interface, there must be a way for the voter to restore the default settings while preserving the current votes.

Discussion

This requirement allows a voter or election worker who has adjusted the system to an undesirable state to reset all settings with the ballot presented to the voter using the new settings, but still keeping what was selected thus far.

Applies to:	Electronic interfaces
Related requirements:	5.2-F – Preserving votes

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000309

7.1-C – Default contrast

The default contrast ratio must be at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons.

1. For electronic displays for voters and election workers, this is measured as a luminosity contrast ratio between the foreground and background colors of at least 10:1.
2. For paper ballots and other paper records, the contrast ratio will be at least 10:1 as measured based on ambient lighting of at least 300 lx.

Discussion

For example, this applies to:

- candidate names,
- a broken arrow,
- the outline of an oval, circle, or rectangular target used to mark voter selections, or
- informational icons identifying voter selections or other information.

Purely decorative elements that do not communicate meaning do not have to meet this requirement.

A 10:1 luminosity contrast ratio provides enough difference between the text and background to enable people with most color vision deficiencies to read the ballot. This is higher than the highest contrast requirements of 7:1 in WCAG 2.0 Checkpoint 1.4.6 (Level AAA) to accommodate a wider range of visual disabilities. There are many free tools available to test color luminosity contrast using the WCAG 2.0 algorithm.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Electronic interfaces

7.1-D – Contrast options

The voting system must provide options for high and low contrast displays, including the alternative display contrast options as listed below:

1. A high contrast option with a white background and dark text, with a luminosity contrast ration of at least 20:1.
2. A high contrast option with a black background (between #000000 and #111111) and one of the following foreground options, including:
    a. yellow text similar to #FFFF00, providing a contrast ratio of at least 17.5:1,
    b. cyan text similar to #00FFFF, providing a contrast ratio of at least 15:1, and

AMERICAN OVERSIGHT

c. white text similar to #FAFAFA, providing a contrast ratio of at least 18:1.

3. A low contrast option, providing a contrast ratio in the range of 4.5:1 to 8:1.

Discussion

This requirement for options for the overall display contrast ensures that there is an option for the visual presentation for people whose vision requires either high or low contrast.

High and low contrast options apply to the entire screen, including decorative elements.

Examples of color combinations for a low contrast options include:

- brown text similar to #BB9966 on a black background (7.8:1),
- black text on a background with text similar to #BB9966 (7.8:1),
- grey text similar to #6C6C6C on a white background (5.2:1),
- grey/brown text similar to #97967E on a black background (6.9:1), and
- grey text similar to #898989 on a dark background similar to #222222 (4.5:1).

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Applies to: Electronic interfaces

7.1-E – Color conventions

The use of color by the voting system must follow these common conventions:

1. Green, blue, or white is used for general information or as a normal status indicator;
2. Amber or yellow is used to indicate warnings or a marginal status; and
3. Red is used to indicate error conditions or a problem requiring immediate attention.

7.1-F – Using color

Color coding must not be used as the only means of communicating information, indicating an action, prompting a response, distinguishing a visual element, or providing feedback on voter actions or selections.

Discussion

While color can be used for emphasis, some other non-color design element is also needed. This could include shape, lines, words, text, or text style. For example, an icon for “stop” can be red enclosed in an octagon shape. Or, a background color can be combined with a bounding outline and a label to group elements on the ballot.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000311

7.1-G – Text size (electronic display)

A voting system's electronic display must be capable of showing all information in a range of text sizes that voters can select from, with a default text size at least 4.8 mm (based on the height of the uppercase I), allowing voters to both increase and decrease the text size.

The voting system may meet this requirement in one of the following ways:

1. Provide continuous scaling with a minimum increment of 0.5 mm that covers the full range of text sizes from 3.5 mm to 9.0 mm.
2. Provide at least four discrete text sizes, in which the main ballot options fall within one of these ranges.
    a. 3.5-4.2 mm (10-12 points)
    b. 4.8-5.6 mm (14-16 points)
    c. 6.4-7.1 mm (18-20 points)
    d. 8.5-9.0 mm (24-25 points)

Discussion

The text size requirements have been updated from the *VVSG 1.1 [VVSG2015]* requirement to better meet the needs of voters who need larger text, including older voters, voters with low literacy, and voters with some cognitive disabilities.

This requirement also fills a gap in the text sizes required in *VVSG 1.1* which omitted text sizes needed or preferred by many voters. Although larger font sizes assist most voters with low vision, certain visual disabilities such as tunnel vision require smaller text.

The sizes are minimums. These ranges are not meant to limit the text on the screen to a single size. The text can fall in several of these text sizes. For example, candidate names or voting options might be in the 4.8-5.6 mm range, secondary information in the 3.5-4.2 mm range, and titles or button labels in the 6.4-7.1 mm range.

The default text size of 4.8 mm is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to:	Electronic interfaces
Related requirements:	5.2-A – No bias 5.2-F – Preserving votes 7.2-D – Scrolling 7.3-B – No split contests

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000312

7.1-H – Scaling and zooming (electronic display)

When the text size is changed, all other information in the interface, including informational icons, screen titles, buttons, and ballot marking target areas, must change size to maintain a consistent relationship to the size of the text. Informational elements in the interface do not have to be scaled beyond the size of the text.

1. When the text is enlarged up to 200% (or 7.1 mm text size), the ballot layout must adjust so that there is no horizontal scrolling or panning of the screen.
2. When the text is enlarged more than 200%, there may be horizontal scrolling or panning if needed to maintain the layout of the ballot and a consistent relationship between the text for ballot options and associated marking targets.

Discussion

The intention of this requirement is that all of the informational elements of the interface change size in response to the text size. However, some interface designs include elements that are already large enough that making them larger would distort the layout. In this case, this does not require those elements to grow proportionately beyond the size of the text.

Techniques for managing scaling and zooming an electronic interface while adjusting the layout to fit the new size are sometimes called responsive design or responsive programming.

This requirement does not preclude novel approaches to on-screen magnification such a zoom lens showing an enlarged view of part of a screen (as long as it meets the requirements in 7.2 for the operability of the controls).

This requirement follows WCAG 2.0 [WCAG10] in requiring scaling with no horizontal scrolling up to 200% and allowing zooming with horizontal scrolling for larger text.

Applies to:	Electronic interfaces
Related requirements:	5.1-A – Voting methods and interaction modes 5.2-A – No bias 5.2-C – All information in all modes 5.2-F – Preserving votes 7.1-G – Text size (electronic display) 7.2-D – Scrolling

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000313

7.1-I – Text size (paper)

The voting system must be capable of printing paper ballots and other paper records with a font size of at least 3.5 mm (10 points).

Discussion

Although the system can be capable of printing in several font sizes, local or State laws and regulations can also govern the use of various font sizes.

If the voting system includes a large-print display option, a good range for the text size is 6.4-7.1 mm matching the size in *7.1-G – Text size (electronic display)*

If typography changes such as text size or display style are used to differentiate languages on a multi-lingual ballot, the requirements in *5.2-A – No bias* (and relevant state election law for ballot design) still apply.

Applies to:	Printed Material
Related requirements:	5.1-E – Reading paper ballots
	7.1-G – Text size (electronic display)

7.1-J – Sans-serif font

The voting system must be capable of presenting text intended for the voter in a sans-serif font.

Discussion

This requirement ensures that systems are capable of best practice while allowing them to also meet local or state laws or regulations that might differ.

In general, sans-serif fonts are easier to read on-screen, look reasonably good when their size is reduced, and tend to retain their visual appeal across different platforms. Examples of sans-serif fonts with good readability characteristics include Arial, Calibri, Microsoft Tai Le, Helvetica, Univers, Clearview ADA, or Open Sans.

WCAG 2.0 [W3C10] and *Section 508 [USAB18]* require that at least one mode of characters displayed on the screen be a sans-serif font.

7.1-K – Audio settings

The voting system's audio format interface must meet the following requirements:

1. The settings for volume and rate of speech are followed regardless of the technical means of producing audio output.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000314

2. The default volume for each voting session is set between 60 and 70 dB SPL.
3. The volume is adjustable from a minimum of 20 dB SPL up to a maximum of 100 dB SPL, in increments no greater than 10 dB.
4. The rate of speech is adjustable throughout the voting session while preserving the current votes, with 6 to 8 discrete steps in the rate.
5. The default rate of speech is 120 to 125 words per minute (wpm).
6. The range of speech rates supported is from 60-70 wpm to 240-250 wpm (or 50% to 200% of the default rate), with no distortion.
7. Adjusting the rate of speech does not affect the pitch of the voice.

Discussion

The top speech rate is slower than some audio users prefer for narrative reading to ensure that candidate names are pronounced clearly and distinctively.

Note that calculation of rate of speech can vary based on the length of the words in the sample, so requirements are stated as a small range.

Speech rates as slow as 50 wpm and as fast as 300 wpm can be included if this can be done without distortion or flanging.

This requirement is intended to be tested using "real ear" measurements not simply measurements at the point of the audio source.

According to an explanation written by the Trace Center *[TC04]*, 60 dB SPL is the volume of ordinary conversation.

FCC regulations for hearing aids, *47 CFR Parts 20 and 68: Hearing Aid Standard [FCC18]*, includes useful information about how to test audio volume and quality.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

Related requirements: 7.1-A – Reset to default settings

7.1-L – Speech frequencies

The voting system's audio format interface must be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

Discussion

The required frequencies include the range of normal human speech. This allows the reproduced speech to sound natural.

AMERICAN OVERSIGHT

This is a requirement for the capability of the system so that it is possible to create intelligible audio. It is not a requirement for a ballot in a real election, which is outside of the scope of the VVSG.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

7.1-M – Audio comprehension

The voting system's audio format interface must be capable of presenting audio content so that it is comprehensible to voters who have normal hearing and are proficient in the language with:

1. proper enunciation, normal intonation, accurate pronunciation in the context of the information, and the capability to pronounce candidate names as intended;
2. low background noise; and
3. recording or reproduction in dual-mono, with the same audio information in both ears.

Discussion

This requirement covers both recorded and synthetic speech. It applies to those aspects of the audio content that are inherent to the voting system or that are generated by default. To the extent that election officials designing the ballot determine the audio presentation, it is beyond of the scope of this requirement.

Support for non-written languages and low literacy includes audio output that is usable by voters who can see the screen.

The International Telecommunications Union (ITU) provides a set of freely available test signals for testing audio quality in *Rec. ITU-T P.50 Appendix I [ITU19]*.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000316

7.1-N – Tactile keys

Mechanically operated controls, buttons, keys, or any other hardware interfaces (including dual switches or sip-and-puff devices) on the voting system available to the voter must**:**

1. be tactilely discernible without activating those controls or keys;
2. include a Unified English Braille, Contracted label if there is a text label; and
3. not require sequential, timed, or simultaneous presses or activations, unless using a full keyboard.

Discussion

A blind voter can operate the voting system by “feel” alone. This means that vision is not necessary for such operations as inserting a smart card or plugging into a headphone jack.

Controls that are distinguished only by shape without a text label do not need a Braille label.

Controls do not depend on fine motor skills.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 7.2-E – Touch screen gestures
7.2-H – Accidental activation
7.2-R – Control labels visible
7.3-L – Icon labels

7.1-O – Toggle keys

The status of all locking or toggle controls or keys (such as the "shift" key) for the voting system available to the voter must be visually discernible, and also discernible through either touch or sound.

Discussion

This applies to any physical controls or keys that have a locking or toggle function.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

7.1-P – Identifying controls

Buttons and controls for the voter that perform different navigation or selection functions must be distinguishable by both shape and color for visual and tactile perception.

Well-known arrangements of groups of keys may be used only for their primary purpose. For example, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000317

Discussion

This applies to buttons and controls implemented either on-screen or in hardware. For on-screen controls, shape includes the label on the button. Redundant cues help those with low vision. They also help individuals who have difficulty reading the text on the screen, those who are blind but have some residual vision, and those who use the controls on a voting system because of limited dexterity. While this requirement primarily focuses on those with low vision, features such as tactile controls and on-screen controls intended primarily to address one kind of disability often assist other voters as well. The Trace Center's EZ Access design is an example of button functions distinguishable by both shape and color *[TCnd].*

Some examples are:

- Color can be helpful to make different sets of functions visually distinct: groups of buttons can share a color, such as Volume UP/DOWN.
- Tactile perception requires different shapes, so that finding a control does not rely solely on the layout: all the shapes cannot be squares, but two or four triangles can be used if they point in different directions.
- As a group of well-known keys, a full alphabetic keyboard is acceptable for entering a write-in candidate name, but individual keys cannot be used for navigation or selection. Using these keys for functions would require a voter to see the visual labels or know the arrangement for those functions.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000318

7.2 – Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.2-A – Display and interaction options

The voting system must provide at least the following display format and interaction mode options to enable voters to mark their ballot to vote, and verify and cast their ballot, supporting the full functionality in each mode:

1. Visual format;
2. Enhanced visual format;
3. Audio format;
4. Touch mode; and
5. Limited dexterity mode.

Discussion

Voters need to be able to choose the combination of display formats and types of controls that work for them, for example, combining the audio format with the tactile mode.

Limited dexterity mode controls include those that do not require dexterity and those that can be operated without use of hands.

Full functionality includes at least instructions and feedback regarding:

- on how to use accessibility features and setting;
- on a change in the display format or control options;
- for navigating the ballot;
- for contest options, including write-in candidates;
- on confirming and changing votes; and
- on final ballot submission.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 5.1-A – Voting methods and interaction modes
5.2-A – No bias

7.2-B – Navigation between contests

The electronic ballot interface must provide navigation controls that allow the voter to advance to the next contest or go back to the previous contest before completing their vote.

AMERICAN OVERSIGHT

Discussion

For example, voters are not forced to proceed sequentially through all contests before going back to check their votes within a previous contest.

This requirement applies whether the voter is using the visual or audio format, or synchronized audio and visual.

As with all requirements, this applies to all display formats and interaction modes.

Related requirements: 7.2-A – Display and interaction options

7.2-C – Voter control

An electronic ballot interface must give voters direct control over making or changing vote selections within a contest. This requirement includes the following:

1. In a vote-for-one contest, selecting a candidate may deselect a previously selected candidate, but the system must announce the change in audio and visual display.
2. In a vote-for-N-of-M contest, the system must not deselect any candidate automatically.
3. In a vote-for-N-of-M contest, the system must inform the voter that they have attempted to make too many selections and offer an opportunity to change their selections.
4. Ballot options intended to select a group of candidates, such as straight-party voting, must provide clear feedback on the result of the action of selecting this option.
5. Ballots with preferential or ranking voting methods must not re-order candidates except in response to an explicit voter command.

Discussion

This requirement covers any selection, de-selection, or change to ballot options. It can be met in a variety of ways, including notifications or announcements of the action the system is taking. For example, if a voter attempts to mark a selection for more candidates than allowed, the system does not take an independent action to de-select a previously selected candidate, but instead notifies the voter of the problem and offers ways to correct it.

As with all requirements, this applies to all display formats and interaction modes.

This requirement addresses situations in which the voter cannot see the change take effect because the previously selected candidate is on another screen, has scrolled off the visible display area, or is out of the voter's field of vision. It is particularly important to voters using the audio format and no

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000320

visual display because they often do not have a way to know that a change that occurs higher up in the contest has taken place.

Examples of feedback include visual changes on the screen and related sounds or messages in text and audio. For example, selecting a candidate is often announced visually with a check-mark image and in audio by naming the candidate selected.

If there is a visual change or announcement about the number of candidates selected (or selections still available), for example, the audio says "you have selected the maximum number of candidates in this contest" in a vote-for-N contest.

An example of feedback on the result of a complex action, such as making a selection in straight-party voting, might be a message confirming the party whose candidates were selected, or even the number of candidates and contests affected by the voter's action.

Related requirements: 7.2-A – Display and interaction options
7.3-E – Feedback
7.3-F – Correcting the ballot

7.2-D – Scrolling

If the number of candidates or length of the ballot question means that the contest does not fit on a single screen using the voter's visual display preferences, the voting system must provide a way to navigate through the entire contest.

1. The voting system may display the contest by:
    a. *pagination* - dividing the list of candidates or other information into "chunks," each filling one screen and providing ways for the voter to navigate among the different chunks; or
    b. *scrolling* – keeping all of the content on a single long display and providing controls that allow the voter to scroll continuously through the content.
2. For either display method, the voting system interface must:
    a. have a fixed header or footer that does not disappear, so voters always have access to navigation elements, the name of the current contest, and the voting rules for the contest;
    b. include easily perceivable cues in every display format to indicate that there is more information or there are more contest options available; and
    c. include an option for an audio format and visual format that sync during scrolling.
3. The navigation method must ensure that the voting system:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000321

a. meets all requirements for providing feedback to the voter;

b. accurately issues all warnings and alerts including notifications of undervotes and overvotes;

c. meets all requirements for control size and interaction, and keeping all controls visible;

d. does not rely only on conventional platform scroll bars; and

e. provides an opportunity to review and correct selections before leaving the contest.

Discussion

The ability to scroll through a list of candidates on a single logical page can be particularly important when a voter selects larger text or is using the audio format.

Information elements that need not scroll might include the name of the contest ("City Council Member"), the voting rules ("vote for 1") and general controls including preference settings or navigation between contests.

A scrolling interface that meets this requirement offers voters a combination of easily perceivable controls or gestures to navigate through the list of candidates or text of a ballot question. For example:

- Navigation within the contest does not rely on knowledge of any particular computer platform or interface standard.
- Navigation within the contest does not only rely on conventional platform scroll bars, which operate differently on two of the major commercial computer platforms.
- Controls have visible labels that include words or symbols.
- Controls are located in the voter's visual viewing area at the bottom (or top) of the scrolling area, for example in the center of the column of names or paragraph of text. This is especially helpful for people with low digital or reading literacy.
- Controls are identified in the audio format and can be activated in all interaction modes.

This overall requirement relates to *7.1-G – Text size (electronic display), 7.1-H – Scaling and zooming (electronic display),* and *7.3-B – No split contests*

The controls used to meet this requirement also need to meet all other requirements including *7.2-H – Accidental activation, 7.2.I – Touch area size, 7.2-F – Voter speech,* and *7.2-E – Touch screen gestures.*

Meeting requirements for notifications relates to *7.3-E – Feedback*, *7.3-F – Correcting the ballot*, *7.3-H – Overvotes, 7.3-I – Undervotes*, and *7.3-K – Warnings, alerts, and instructions*.

Applies to: Electronic interfaces

AMERICAN OVERSIGHT

Related requirements: 7.1-G – Text size (electronic display)
7.1-H – Scaling and zooming (electronic display)
7.2-E – Touch screen gestures
7.2-F – Voter speech
7.2-H – Accidental activation
7.2.I – Touch area size
7.3-B – No split contests
7.3-E – Feedback
7.3-F – Correcting the ballot
7.3-H – Overvotes
7.3-I – Undervotes
7.3-K – Warnings, alerts, and instructions

7.2-E – Touch screen gestures

Voting system devices used by voters with a touch screen may use touch screen gestures (physical movements by the user while in contact with the screen to activate controls) in the interface if the following conditions are met:

1. Gestures are offered as another way of interacting with a touch screen and an optional alternative to the other touch interactions.
2. Gestures work consistently across the entire voting interaction.
3. Gestures do not include navigation off the current contest.
4. Gestures are used in a way that does not create accidental activation of an action through an unintended gesture.
5. Gestures are limited to simple, well-known gestures.
6. Gestures do not require sequential, timed or simultaneous actions.

Discussion

This requirement ensures that the use of gestures does not interfere with the accessibility features of the voting system or make the interface difficult to use by relying on an interaction mode with no easy way to make them perceivable in the visual or audio formats.

In relying on simple and common gestures, this requirement does not intend to fully duplicate the gestures for commercial mobile platforms used with an audio format for accessibility.

Tapping (touching the screen briefly) is the most basic gesture and is used on all touch screens. Other commonly used gestures include:

- pinching or spreading fingers to zoom,
- swiping to scroll, and

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000323

- pressing and holding to drag

Examples of gestures that require sequential or simultaneous actions are double-tapping, 2, 3 or 4 finger swiping, touch and hold for a set period of time, or those that require coordinated actions with fingers on both hands. On desktop systems, assistive preference options like Sticky Keys can make these complex gestures accessible, but they require familiarity beyond what is acceptable in a voting system.

Examples of timed gestures include differentiating between long and short touches, or which require touching twice in rapid succession to highlight and then activate the button or selection.

Applies to:	Electronic interfaces
Related requirements:	7.1-N – Tactile keys
	7.2-H – Accidental activation

7.2-F – Voter speech

If the voting system includes speech or human sounds as a way for voters to control the system:

1. it must not require the voter to speak recognizable voting selections out loud, and
2. speech input must not be the only non-visual interaction mode.

Discussion

This requirement allows the use of speech input as long as voters can choose other ways of interacting with the voting system that do not require either vision or use of their hands.

It is also important to consider how speech would work as a way of voting in a noisy polling place environment.

Related requirements:	6.1-A – Preserving privacy for voters
	6.1-D– Audio privacy

7.2-G – Voter control of audio

The voting system must allow the voter to control the audio format including:

1. pausing and resuming the audio;
2. repeating any information;
3. skipping to the next or previous contest; and
4. skipping over the reading of the ballot question text.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000324

These features can also be useful to voters with cognitive disabilities.

This is comparable to the ability of sighted voters to:

- move on to the next contest once they have made a selection or to abstain from voting on a contest altogether, or
- skip over the wording of a referendum on which they have already made a decision prior to the voting session (for example, "Vote yes on proposition #123").

Applies to: Electronic interfaces

7.2-H – Accidental activation

Both on-screen and physical controls on the voting system must be designed to prevent accidental activation.

Discussion

There are at least two kinds of accidental activation:

- When a control is activated to execute an action as it is being “explored” by the voter because the control is overly sensitive to touch.
- When a control is in a location where it can easily be activated unintentionally. For example, when a button is in the very bottom left corner of the screen where a voter might hold the unit for support.

The draft of WCAG 2.1, the next version of *WCAG 2.0 [W3C10]* includes a similar requirement and offers guidelines for preventing accidental activation including that the activation be on the release of the control (an “up-event”) or equivalent, or that the system provides an opportunity to confirm the action.

In addition to the accessibility needs for preventing accidental activation, it can be an issue if voters perceive the voting system as changing their voting selections.

Related requirements: 7.1-N – Tactile keys
7.2-E – Touch screen gestures

7.2-I – Touch area size

If the voting system has a touch screen, the touch target areas must:

1. be at least 12.7 mm **(**0.5 inches) in both vertical and horizontal dimensions;
2. be at least 2.54 mm (0.1 inches) away from adjacent touch areas; and

AMERICAN OVERSIGHT

3. not overlap another touch area.

Discussion

The requirements for touch size areas on voting systems are larger than commercial standards for mobile devices:

- to ensure that the touch areas are large enough for voters with unsteady hands;
- to ensure that voting systems allow full adjustment to the most comfortable posture; and
- to allow for touch screens that do not include advanced algorithms to detect the center point of a touch.

The required touch area size is larger than some of the commercial standards for mobile phones to allow for use by voters with limited dexterity.

The required marking area size is within sizes suggested in the draft WCAG 2.1 (the next version of *WCAG 2.0 [W3C10]*) for target areas that accept a touch action.

An MIT Touch Lab study of **Human Fingertips to Investigate the Mechanics of Tactile Sense** found that the average human finger pad is 10-14 mm and the average fingertip is 8-10 mm.

Applies to: Touch screen interfaces

7.2-J – Paper ballot target areas

On a paper ballot that a voter marks by hand, the area of the target used to mark a voting selection must be at least 3 mm (0.12 inches) across in any direction.

Discussion

This requirement applies to marking ovals, circles, squares, or other optical scan ballot designs.

Although the marking target for hand-marked paper ballots needs to be large enough to see, a target that is too large can also make it hard to fill in the area completely.

Applies to: Paper ballots

7.2-K – Key operability

Physical keys, controls, and other manual operations on the voting station must be operable with one hand and not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys must be no greater than 5 lbs. (22.2 N).

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000326

Discussion

Voters can operate controls without excessive force. This includes operations such as inserting an activation card and inserting and removing ballots.

This does not apply to on-screen controls.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Physical controls

7.2-L – Bodily contact

The voting station controls must not require direct bodily contact or for the body to be part of any electrical circuit. If some form of contact is required, a stylus or other device with built-in permanent tips will be supplied to activate capacitive touch screens.

Discussion

This requirement ensures that controls and touch screens can be used by individuals using prosthetic devices or that it is possible to use a stylus on touch screens for either greater accuracy or limited dexterity input.

One type of touch screen – capacitive touch panels – rely on the user's body to complete the circuit. They can be used if manufacturers supply a stylus or other device that activates the capacitive screen.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Applies to: Electronic interfaces

7.2-M – No repetitive activation

Voting system keys or controls must not have a repetitive effect when they are held in an active position.

Discussion

This is to preclude accidental activation. For instance, if a voter is typing in the name of a write-in candidate, depressing and holding the "e" key results in only a single "e" added to the name.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

7.2-N – System response time

The voting system's response time must meet the following response times:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000327

1. The system initially responds to a voter action in no more than:
    a. 0.1 seconds for a visual change, and
    b. 0.5 seconds for an audio response.
2. The system responds to a voter marking a vote in no more than 1 second for both a visual response and an initial audio response.
3. The system completes the visual response or display in no more than 1 second or displays an indicator that a response is still being prepared.

Discussion

This is so the voter can very quickly perceive that an action has been detected by the system and is being processed. The voter never gets the sense of dealing with an unresponsive or "dead" system. Note that this requirement applies to both auditory and visual voting system responses.

For example, if the voter touches a button to indicate a vote for a candidate, a visual system might display an "X" next to the candidate's name, and an audio system might announce, "You have voted for John Smith for Governor". Even for "large" operations such as initializing the ballot or painting a new screen, touch screen system ideally should not take more than 10 seconds.

In the case of audio systems, no upper limit is specified, since certain operations can take longer, depending on the length of the text being read (for example, reading out a long list of candidates running in a contest). For instance, the system might present a progress bar indicating that it is "busy" processing the voter's request. This requirement is intended to preclude the "frozen screen" effect, in which no detectible activity is taking place for several seconds. There need not be a specific "activity" icon, as long as some visual change is apparent (such as progressively "painting" a new screen or providing audio feedback).

Applies to: Electronic interfaces

7.2-O – Inactivity alerts

If the voter has not interacted with the voting system for a long time, that is, between 2-5 minutes, the system must notify the voter and meet the following requirements:

1. The system must document the inactivity time.
2. When the voter’s inactivity time expires, the electronic ballot interface must issue an alert and provide a way for the voter to receive additional time.
3. The alert time must be between 20 and 45 seconds.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000328

4. If the voter does not respond to the alert within the alert time, the electronic ballot interface must go into an inactive state requiring election worker intervention.

Discussion

Each type of system will have a given inactivity time that is consistent among and within all voting sessions. This ensures that all voters are treated equitably.

For a referendum, in audio format, the timer starts when the audio finishes.

Applies to: Electronic interfaces

7.2-P – Floor space

When used according to the manufacturer's installation instructions, the voting station must allow floor space for voters using a wheelchair or a voter's assistant by:

1. providing a clear area for a wheelchair of 760 mm (30 inches) wide and 1220 mm (48 inches) deep, and
2. providing adequate room for a voter's assistant, including enough room for both the voter and an assistant to enter the area of the voting station.

Discussion

This requirement sets minimum dimensions for clear floor space around a voting station and ensures that the manufacturer's voting station design and associated installation instructions support polling place layouts that can achieve this requirement.

In planning a polling place layout, election officials should consult the *U.S Access Board Technical Guide: Clear Floor or Ground Space and Turning Space [USAB14a]* and the *U.S. Department of Justice ADA Checklist for Polling Places [USDOJ16]* to be sure that a voter using a wheelchair can reach the voting station. They should also consider space needed if a voter's assistant also uses a mobility device.

7.2-Q – Physical dimensions

The physical dimensions of the voting station must meet the U.S. Access Board requirements in *Appendix A* to *Part 1194 – Section 508* of the *Rehabilitation Act: Application and Scoping Requirements, Chapter 4: Hardware, Section 407.8 Operable Parts: Reach Height and Depth [USAB14b].*

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000329

This requirement is part of *Section 508 [USAB18]*. with the text of the requirements for reach height and depth with illustrations in the "#407 operable parts" section.

Many voting systems can be set up in a variety of ways for use in a polling place or vote center. For example, a system might sit on a table that allows voters to put their legs under the table in a polling place, but on a counter with no legroom in a vote center. Wheelchairs and scooters also allow voters different abilities to reach controls, and the voter might approach the voting system from the front or side, depending on the physical design and how it is presented to the voter.

A guide to meeting the requirements in the ADA standard for ensuring that voters can reach and us all operable parts can be found at *[USAB14b]*.

7.2-R – Control labels visible

Labels for physical controls used by voters must be placed:

1. on a surface of the voting system where voters can see them from a seated or standing posture, and
2. within the dimensions required in *7.2-Q – Physical dimensions*.

Discussion

This requirement ensures that voters can find controls, even if they are placed on a side or top surface of the voting system, and that blind voters can discover any Braille labels associated with the text label by touch.

Related requirements: 7.1-N – Tactile keys
7.2-Q – Physical dimensions
7.3-L – Icon labels

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000330

7.3 – Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

7.3-A – System-related errors

The voting system must help voters complete their ballots effectively, ensuring that the features of the system do not lead to voters making errors during the voting session.

Discussion

This requirement provides a general scope that supports the other requirements in 7.3. It is meant to encourage innovation in meeting this principle while ensuring that any new design features not covered explicitly in 7.3 help and not hinder voters in understanding and voting their ballots effectively.

7.3-B – No split contests

The voting system must have the capability of displaying a ballot so that no contest is split into two groups of options.

1. For paper ballot formats, the system must include a way of presenting a contest that does not divide the options across two columns or two pages.
2. For electronic interfaces, if a contest does not fit onto one screen view, the system must include a way to meet the requirements in *7.2-D – Scrolling* for managing the way the list of options is displayed.

Discussion

There is strong evidence from recent elections that when a contest is split into two or more sections, there is a risk that the voter can perceive one contest as two (and overvote), or fail to see all of the contest options (and vote for a candidate other than the one they intend to).

This a requirement for a capability of the ballot design or election management tools for the voting system to allow election officials to lay out a ballot with good usability.

Related requirements: 7.2-D – Scrolling

7.3-C – Contest information

All ballots must clearly indicate the office or question title and the maximum number of choices allowed for each contest.

AMERICAN OVERSIGHT

1. In an electronic ballot marking interface, the information for each contest includes, in a consistent order: The title of the office or ballot question, including any distinguishing information such as the length of the term or the jurisdiction.
2. The maximum number of selections allowed in the contest.
3. In the audio format only, the number of options or candidates.
4. If any selections have already been made, the number of selections remaining.
5. In the audio format only, if any selections have been made, the currently selected candidates or options.
6. Any instructions or reminders of how to find marking instructions, placed visually and in audio after the contest information.

Discussion

This requirement is intended to work with any relevant state election laws or regulations for ballot design.

For voters using audio features, best practice is to announce how many candidates or voting options are available, providing an audio cue similar to a visual scan of the ballot in a similar way to assistive technology such as screen readers.

Placing basic instructions last helps voters using the audio format know when they can skip to making selections in the contest without missing any important information.

7.3-D – Consistent relationship

The relationship between the name of a candidate or other voting option and the way the voter marks that selection, including the spatial relationship in the ballot layout, must be consistent throughout the ballot for each type of contest.

Discussion

A type of contest includes contests to:

- vote for one or more candidates,
- answer a ballot question,
- vote whether to retain a judge,
- indicate preferential ranking of candidates, or
- make a selection in other contests with distinct voting methods.

This requirement ensures that the mechanism for marking a selection in a contest to elect one or more candidates to an office is not to the left of some candidates' names and to the right of others.

AMERICAN OVERSIGHT

If there is more than one spatial relationship, the difference should not be contradictory or confusing to a voter when combined on a single ballot.

Related requirements: 2.2-A – User-centered design process
5.2-A – No bias
7.3-N – Instructions for voters
8.3-A – Usability tests with voters

7.3-E – Feedback

The voting system must provide unambiguous feedback confirming the voter's selection.

Discussion

This requirement applies to electronic interfaces because on paper ballots the voter supplies the mark to indicate a selection, not the voting system. For example, the system can display a checkmark beside the selected option or conspicuously change its appearance.

This requirement also applies to the audio format. It is especially important that the way the status of the process of making selections is announced in the audio format is unambiguous. For example, the phrase "is selected" and "de-selected" can sound similar, especially at faster audio speeds. Choosing phrases that are more distinct, paying attention to the audio phrasing, and testing with the maximum audio speed can help avoid this problem.

Designers of paper ballots that include straight-party voting should test feedback features carefully to ensure that voters can understand the scope of their selection and the ballot options it affects.

Applies to: Electronic interfaces

Related requirements: 7.2-C – Voter control
7.3-G – Full ballot selections review

7.3-F – Correcting the ballot

The voting system must provide the voter the opportunity to correct the ballot before it is cast and counted.

An electronic ballot interface must:

1. allow the voter to change a vote within a contest before advancing to the next contest;
2. provide the voter the opportunity to correct the ballot before it is cast or printed; and
3. allow the voter to make these corrections without assistance.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000333

For paper ballots, this can be achieved through appropriately placed written instructions, including requiring the voter to obtain a new paper ballot to correct a mistake.

Vote-by-mail ballots can have different instructions for making corrections from those cast in-person.

Some voting methods allow a voter to print a replacement ballot, as long as they only cast one.

Also, note the requirements for both electronic ballot interfaces and scanners and precinct-count optical scanners in *7.3-H – Overvotes* and in *7.3-I – Undervotes.*

This requirement supports *HAVA [HAVA02]*.

Related requirements: 5.2-F – Preserving votes
7.3-H – Overvotes
7.3-I – Undervotes

7.3-G – Full ballot selections review

A voting system with an electronic voting interface must provide the voter with a function to review their selections before printing or casting their ballot that:

1. displays all of the contests on the ballot with:
    a. the voter's selections for that contest,
    b. a notification that they have not made a selection, or
    c. a notification that they have made fewer selections than allowed;
2. offers an opportunity to change the selections for a contest and return directly to the review screen to see the results of that change; and
3. allows the voter to continue to the function for casting the ballot without making a correction at any time in the review process.

The review function may also be provided on a scanner or other device where the voter marks and casts a paper ballot.

Discussion

This requirement is an implementation of the *HAVA [HAVA02]* requirement that voters be able to review and change their ballot before casting.

Electronic interfaces are required to prevent overvotes. This is usually done while originally marking a contest, so there are no overvoted contests to display on the review screen.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000334

Including a review screen on a scanner that accepts ballots marked by hand gives those voters an opportunity to review how their ballot will be read by the scanner and make any corrections before casting the ballot.

Related requirements:	5.2-F – Preserving votes 7.3-H – Overvotes 7.3-I – Undervotes

7.3-H – Overvotes

The voting system must notify the voter if they attempt to select more than the allowable number of options within a contest (overvotes) and inform them of the effect of this action before the ballot is cast and counted.

1. An electronic ballot interface must prevent voters from selecting more than the allowable number of options for each contest.
2. A scanner or other device that a voter uses to cast a paper ballot must be capable of providing feedback that identifies specific contests that have been overvoted in visual format, and with either audio format or sound cues.

Discussion

This requirement does not specify exactly how the system will respond when a voter attempts to select an "extra" candidate. For instance, the system can present the warning, or, in the case of a single-choice contest (vote for 1), simply change the vote selection and issue a warning.

For electronic ballot interfaces, this requirement does not allow disabling the features that prevent overvotes.

Voters marking paper ballots can be informed of the effect of overvoting through appropriately placed instructions.

This requirement supports *HAVA [HAVA02]*.

Applies to:	Electronic interfaces and ballot scanners
Related requirements:	5.1-D – Accessibility features 7.2-C – Voter control 7.3-K – Warnings, alerts, and instructions

7.3-I – Undervotes

The voting system must notify voters in both visual and audio formats of the specific contest in which they select fewer than the allowable number of options (that is, for undervotes).

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000335

1. Both electronic interfaces and scanners must allow the voter to submit an undervoted ballot without correction.
2. The voting system may allow election officials to disable the notification of undervotes on a scanner.

Discussion

For electronic interfaces, this notification can be incorporated into the review feature.

This requirement supports *HAVA [HAVA02]*.

Applies to:	Electronic interfaces and scanners
Related requirements:	7.2-C – Voter control
	7.3-K – Warnings, alerts, and instructions

7.3-J – Notification of casting

1. The voting system must notify the voter in both visual and audio format whether their ballot was successfully or unsuccessfully cast. If a ballot is not successfully cast (that is, the device did not complete the documented procedures for the system, including reading a paper ballot, recording an electronic image or record, or transporting the ballot to a ballot box), the voting device must notify the voter and provide clear instruction as to the steps the voter needs take to cast the ballot.
2. A scanning device must be capable notifying the voter that they have cast a paper ballot that is blank on one or both sides. The system may provide a means for an authorized election official to deactivate the notification of a blank ballot.

Discussion

The purpose of this requirement is to provide feedback to voters to assure them that the voting session has been completed. Note that either a false notification of success or a missing confirmation of actual success violates this requirement.

Detecting situations in which the voter might be unaware that the ballot is two-sided and left one side blank is distinct from the ability to detect and warn about undervoting.

At a minimum, this requirement is intended to ensure that blind and low-vision voters receive an audio notification that a ballot is successfully cast. This might be a sound that is the audio equivalent of a waving flag or other visual.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000336

7.3-K – Warnings, alerts, and instructions

Warning, alerts, and instructions issued by the voting system must be distinguishable from other information.

1. Warnings and alerts must clearly state in plain language:
    a. the nature of the issue or problem,
    b. whether the voter has performed or attempted an invalid operation or whether the voting system itself has malfunctioned in some way, and
    c. the responses available to the voter.
2. Each step in an instruction or item in a list of instructions must be separated:
    a. spatially in visual formats, and
    b. with a noticeable pause in audio formats.

Discussion

For instance, “Do you need more time? Select ‘Yes’ or ‘No’.” rather than “System detects imminent timeout condition.” In case of an equipment failure, the only action available to the voter might be to get assistance from an election worker.

Keeping instructions separate includes not "burying" several unrelated instructions in a single long paragraph.

Alerts intended to confirm visual changes to a voter using the audio format (such as confirmation that the screen has been turned on or off) can be communicated in audio, with a short text or sound.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]*.

7.3-L – Icon labels

When an icon is used to convey information, indicate an action, or prompt a response, it must be accompanied by a corresponding label that uses text.

The only exception is that the two 3.5 mm (1/8 inch) jacks for audio and personal assistive technology (PAT) may be labeled with tactilely discernable and visually distinct icons of a headset (for audio) and wheelchair (for the PAT connector) that are at least 13 x 13 mm in size.

Discussion

While icons can be used for emphasis when communicating with the voter, they are not to be the only means by which information is conveyed, since there is no widely accepted "iconic" language,

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000337

and therefore, not all voters might understand a given icon. The exception is based on the *ADA Standards for Accessible Design. Chapter 7 [ADA10]*.

Related requirements: 7.1-N – Tactile keys
7.2-R – Control labels visible
8.1-E – Standard audio connectors
8.1-I – Standard PAT jacks

7.3-M – Identifying languages

A vote-capture device or other voting session device that offers language options to a voter must:

1. visibly present the controls to identify or change language on the screen at all times, not hidden within a help or settings feature, and
2. include the native version of each language name in the list of language options.

Discussion

Voters looking for an option for an alternative language can recognize it more easily as it is written in the language itself.

The English name or spelling can also be used to identify language, along with the native name.

Applies to: Electronic interfaces

7.3-N – Instructions for voters

The voting system must provide voters access to instructions for all its operations at any time during the voting session.

1. For electronic interfaces, the voting system must provide a way for voters to get help directly from the system.
2. For paper ballots, the system must be capable of including on the ballot both text and images with instructions for how to mark the ballot.
3. Voting systems must present instructions near to where they are needed during the voting session.

Discussion

The purpose of this requirement is to minimize voters' need for assistance from an election worker and to permit the voter to verify and cast, privately and independently, the votes selected.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000338

When the system works correctly, the voter will find the help they need from the system when and where they need it. For instance, only general instructions should be grouped at the beginning of the ballot; those pertaining to specific situations should be presented near those situations.

If an operation is available to the voter, it will be documented. Examples include how to make a vote selection, navigate among contests, cast a straight-party vote, cast a write-in vote, adjust display and audio characteristics, or select a language.

Electronic ballot interface systems often provide assistance with a distinctive "help" button.

Instructions can be on the ballot itself or separate from the ballot, as long as the voter can find them easily.

Related requirements: 5.1-F – Accessibility documentation

7.3-O – Instructions for election workers

The voting system must include clear, complete, and detailed instructions and messages for setup, polling, shutdown, and how to use accessibility features.

1. The documentation required for normal voting system operation must be:
    a. presented at a level appropriate for election workers who are not experts in voting system and computer technology, and
    b. in a format suitable for use in the polling place.
2. Printed procedural instructions, and on-screen instructions and messages must enable the election workers to verify that the voting system
    a. has been set up correctly (setup),
    b. is in correct working order to record votes (polling), and
    c. has been shut down correctly (shutdown).

Discussion

This requirement covers documentation for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition. The instructions are usually in the form of a written manual, but can also be presented on other media, such as a DVD or videotape. In the context of this requirement, "message" means information delivered by the system to the election workers as they attempt to perform a setup, polling, or shutdown operation. Specific guidance on how to implement this requirement is contained in *[NIST08]*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000339

For instance, the documentation should not presuppose familiarity with personal computers. And a single large reference manual that simply presents details of all possible operations would be difficult to use, unless accompanied by aids such as a simple "how-to" guide.

It is especially important that election workers and other non-expert workers know how to set up accessibility features which are not used frequently. This will help ensure voters who need these features can vote privately and independently.

Overall, election workers should not have to guess whether a system has been setup correctly. The documentation should make it clear what the system "looks like" when correctly configured.

Related requirements: 5.1-F – Accessibility documentation

7.3-P – Plain language

Information and instructions for voters and election workers must be written clearly, following the best practices for plain language. This includes messages generated by the voting system for election workers in support of the operation, maintenance, or safety of the system.

Discussion

The plain language requirements apply to instructions that are inherent to the voting system or that are generated by default. To the extent that instructions are determined by election officials designing the ballot, they are beyond of the scope of this requirement.

Any legally required text is an exception to this plain language requirement.

Plain language best practices are guidelines for achieving clear communication and include:

- Using familiar, common words and avoiding technical or specialized words that voters are not likely to understand. For example, "There are more contests on the other side" rather than "Additional contests are presented on the reverse."
- Issuing instructions on the correct way to perform actions, rather than telling voters what not to do. For example, “Fill in the oval for your write-in vote to count” rather than, “If the oval is not marked, your write-in vote cannot be counted.”
- Addressing the voter directly rather than use passive voice when giving instructions. For example, "remove and retain this ballot stub" rather than "this ballot stub must be removed and retained by the voter."
- Stating a limiting condition first, followed by the action to be performed when an instruction is based on a condition. For example, use "In order to change your vote, do X", rather than "Do X, in order to change your vote."
- Avoiding the use of gender-based pronouns. For example, "Write in your candidate’s name directly on the ballot" rather than "Write in his name directly on the ballot."

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000340

For specific guidance on how to implement this requirement, see *[NIST09a].* Although part of general usability, using plain language is also expected to assist voters with cognitive disabilities.

Information written in plain language is easier to translate to meet language access requirements.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000341

Principle 8
Robust, Safe, Usable, and Accessible

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities.

8.4 - The voting system is evaluated for usability with election workers.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000342

Principle 8
ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

This principle covers how the voting system performs in use, including physical safety and the usability and accessibility of the complete voting system. The guidelines under *Principle 8* are:

1 - Protect from harmful conditions covers requirements that ensure the voting system is Robust (completing the Web Content Accessibility Guidelines' (WCAG's) organizing principles known as POUR (Perceivable, Operable, Understandable, Robust)) and does not present any harmful conditions to voters and election workers. It addresses how an electronic screen displays information the voter needs and covers personal assistive technology (PAT) and topics such as audio connectors, jacks, hearing aids, and handsets.

2 - Meet accessibility standards explicitly includes the entire federal standard for accessibility, the basis for many of the requirements in *Principle 7* for voting system electronic interfaces. This standard can fill in any gaps the *VVSG 2.0* does not specifically address. This is especially important for the part of the voting system that might use general interfaces, such as a browser-based ballot marking system that runs on personal computers.

3 and 4 - Usability tests require usability testing the voting system to ensure that it not only meets the detailed design requirements but will function well for both voters and election workers in use. Testing with a variety of voters, including those with and without disabilities, ensures the voting system is usable and accessible to all voters. The testing with election workers ensures that he system's setup, polling, and shutdown are relatively easy to learn, understand, and perform.

Principle 8 is related to *Guideline 2.2*, which requires a user-centered design and development process for the entire voting system. It covers election workers and a wide range of representative voters, including those with and without disabilities.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000343

8.1 – The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.1-A – Electronic display screens

If the voting system uses an electronic display screen, the display must have the following characteristics:

1. For all electronic display screens:
    a. antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections, and
    b. minimum uniform diffuse ambient contrast ratio for 500 lx illuminance: 10:1.
2. If the display is the primary visual interface for making vote selections:
    a. minimum diagonal display size: 12 inches, and
    b. minimum display resolution: 1920 x 1080 pixels.
3. If the display screen is for messages to voters or poll workers:
    a. minimum diagonal display size: 7.9 inches, and
    b. minimum display resolution: 1024x768 pixels.

Discussion

Displays that measure larger than the 12-inch diagonal provide the opportunity for ballot layouts that can more easily use large text settings.

Applies to: Electronic interfaces

8.1-B – Flashing

If the voting system emits light in flashes, there must be no more than three flashes in any one-second period.

Discussion

This requirement has been updated to meet *WCAG 2.0 [W3C10]* and *Section 508 [USAB18]* software design issue standards.

Applies to: Electronic interfaces

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000344

8.1-C – Personal Assistive Technology (PAT)

The support provided to voters with disabilities must be intrinsic to the voting system so that a voter's personal assistive devices will not be necessary to operate the voting system correctly.

Discussion

This requirement does not preclude the voting system from providing interfaces to assistive technology. (See definition of "personal assistive devices" in *Appendix A - Glossary*). Its purpose is to ensure that voters are not required to bring special devices with them in order to vote successfully.

This requirement assumes that voters can use their personal headsets, hearing aids, eyeglasses, canes, or other aids they typically have with them.

8.1-D – Secondary ID and biometrics

If a voting system uses biometric measures for identifying or authenticating voters and election workers, it must provide an alternative that does not depend on the same biometric capabilities.

Discussion

For example, if fingerprints are used for voter identification, another mechanism will be provided for voters without usable fingerprints.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

8.1-E – Standard audio connectors

The voting system must provide its audio signal for the audio format interface through an industry standard connector using a 3.5 mm (1/8 inch) stereo headphone jack to allow voters to use their own audio assistive devices for private listening.

Applies to: Electronic interfaces

8.1-F – Discernable audio jacks

The audio jack on any voting station device must be in a location that voters can discover, discernable by touch while sitting or standing in front of the unit, and not located near a sharp edge.

Discussion

For example, if the jack is slightly recessed with a round bezel, it will be easier for voters to identify the jack and to insert the headset plug into it.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000345

8.1-G – Telephone style handset

If the voting system uses a telephone style handset or headphone to provide audio information, it must provide a wireless T-Coil 9 coupling for assistive hearing devices so it provides access to that information for voters with partial hearing, achieving at least a category T4 rating as defined by the *American National Standard Institute (ANSI) for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19-2019 [ANSI19]*.

Discussion

This requirement applies only to telephone style handsets/headphones to ensure their compatibility with assistive hearing devices.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 6.1-D – Audio privacy
8.1-J – Hearing aids

8.1-H – Sanitized headphones

The voting system must be supplied with a means to sanitize headphones or handsets and instructions for election workers on the procedure to ensure that a sanitized headphone or handset is available to each voter.

Discussion

This requirement can be achieved in various ways, including the use of "throwaway" headphones or sanitary coverings.

8.1-I – Standard PAT jacks

A vote-capture device or voter-facing device must provide a 3.5 mm (1/8 inch) industry standard jack voters can use to connect their personal assistive technology switch to the system.

1. The jack must allow only switch activations to be transmitted to the system.
2. The system must accept switch input that is functionally equivalent to other input methods.
3. All the functionality of the voting system must be available through technology using this input mechanism.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000346

This requirement is related to the requirements for low dexterity modes (in *5.1-A – Voting methods and interaction modes* and in *7.2-A – Display and interaction options*). It ensures that voters with very low dexterity, in particular those who do not have the use of their hands can use the vote-capture devices by providing a means for them to connect personal assistive technology (PAT) if they cannot use the supplied touch or tactile input devices.

Examples of personal assistive technology switches include dual switches (sometimes called “adaptive switches” or “jelly switches”) and "sip and puff" devices that communicate as a single key press.

Ideally, the jack will be on the tactile keypad or have some other mechanism to provide sufficient reach to a wheelchair tray or the voter’s lap.

While it is desirable that the voter be able to independently initiate use of the non-manual input mechanism, this requirement guarantees only that the voter can vote independently once the mechanism is enabled.

The PAT jack is separate from the audio jack required in *8.1-F – Discernible audio jacks*, which connects to the audio output provided by the system.

Related requirements: 5.1-A – Voting methods and interaction modes
7.2-A – Display and interaction options

8.1-J – Hearing aids

Voters who use assistive hearing devices must be able to use voting devices as intended:

1. The voting device must not cause electromagnetic interference with assistive hearing devices that would substantially degrade the performance of those devices.
2. The voting device, measured as if it were a wireless device, must achieve at least a category T4 rating as defined by *American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids, ANSI C63.19-2019 [ANSI19].*

Discussion

"Hearing devices" include hearing aids and cochlear implants.

This requirement is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

Related requirements: 8.1-G – Telephone style handset

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000347

8.1-K – Eliminating hazards

Devices associated with the voting system must be certified in accordance with the requirements of *IEC/UL 62368-1 [UL19], Edition 3: Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements* by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.

The certification organization's scope of accreditation is acceptable if it includes *IEC/UL 62368-1 [UL19]*.

Discussion

IEC/UL 62368-1 is a comprehensive standard for IT equipment and addresses all the hazards discussed above under Safety. It replaces *IEC/UL 60950-1 [UL07].*

8.2 – The voting system meets currently accepted federal standards for accessibility.

8.2-A – Federal standards for accessibility

Voting systems must meet federal standards for accessibility, including the version of *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines [USAB18]*, in effect as of January 18, 2018, and the *WCAG 2.0 Level AA checkpoints [W3C10]* included in that standard.

Discussion

This applies to all parts of the voting system including the election management system (EMS).

Section 508 standards apply to electronic and information technology, including computer hardware and software, websites, multimedia, and other technology such as video, phone systems, and copiers. This requirement also supports the ADA *[ADA10].*

Applies to: Electronic interfaces, including EMS

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000348

8.3 – The voting system is evaluated with a wide range of representative voters, including those with and without disabilities.

8.3-A – Usability tests with voters

The manufacturer must conduct usability tests with voters using the voting system, including all voter activities in a voter session from ballot activation to verification and casting.

The test participants must include voters who represent the following:

1. General population, using the visual interface (without audio), including:
    a. voters who are native speakers of the language being tested for each language defined as supported in the technical data package (TDP);
    b. blind voters, using the audio format plus tactile controls;
    c. voters with low vision, using the enhanced visual features with and without audio; and
    d. voters with limited dexterity, using the visual interface with low and no dexterity controls.
2. The manufacturer must submit a report of the results of their usability tests, including effectiveness, efficiency, and satisfaction measures, as part of the TDP using *ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].*

Discussion

Voting system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system.

Related requirements: 2.2-A – User-centered design process
5.1-D – Accessibility features

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000349

8.4 – The voting system is evaluated for usability with election workers.

8.4-A – Usability tests with election workers

The manufacturer must conduct usability tests of the voting system setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.

The tasks to be covered in the test must include:

1. Setup and opening for voting, which involves:
    a. operation during voting;
    b. use of assistive technology or language options that are part of the voting system;
    c. shutdown at the end of a voting day during a multi-day early voting period, if supported by the voting system;
    d. shutdown at the end of voting including running any reports;
    e. providing ballots in different languages;
    f. selecting the correct ballot type (for example, for vote centers); and
    g. setting up the voting system to use different display formats and interaction modes.
2. The test participants must include election workers representing a range of experience.
3. The manufacturer must submit a report of the results of their usability tests, as part of the TDP using *ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports [ISO06b].*

Discussion

Voting system manufacturers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible voting system. This requirement covers the procedures and operations for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as ballot definition or system repair. These "normal" procedures

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000350

should not require any special expertise. The procedures may require a reasonable amount of training, similar to the training generally provided for temporary election workers.

Related requirements: 2.2-A – User-centered design process
7.3-O – Instructions for election workers

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000351

Principle 9
Auditable

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.4 - The voting system supports efficient audits.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000352

Principle 9
AUDITABLE

The voting system is auditable and enables evidence-based elections.

The requirements for *Principle 9* include ensuring that an error in the voting system cannot cause an undetectable change in the election results, that the system produces records that are resilient and can be checked and produces records that enable an efficient compliance audit. Delivery, return, and non-voting equipment process used for vote-by-mail fall out of the scope of the VVSG and is often based on jurisdictional procedure.

The sections in *Guideline 9.1* cover:

1 - Software independence requires that the voting system provide proof that the ballots have been recorded correctly and are compliant within the Paper-based System Architecture or Cryptographic E2E System Architectures. In addition, the manufacturer documents the mechanism used to provide software independence. These requirements ensure that failures in voting system software can be detected and rectified

2 – Tamper-evidence requires the records used to record ballet selections cannot be undetectably altered. These records are needed to enable detection of incorrect election outcomes. They need to capture the voter's ballot selection when each ballot is cast.

3 – Voter verification requires that voting machines allow voters the opportunity to verify that the system correctly interpreted their ballot selections, identify errors with their selections, and restart a voting session if a ballot is unacceptable. Records that protect against software failures only work if voters can verify their selections are correct.

4 – Auditable means the voting system generates records that enable external auditors to verify that ballots are correctly tabulated, even if the system is compromised or there are faults in components. The manufacturer is to provide a procedure to verify that cast records are correctly tabulated.

5 – Paper records covers the requirements that paper-based (not cryptographic end-to-end verifiable) voting systems produce a verifiable paper record of the voter's ballot selection and retain a copy of that selection which has a unique identifier. The voter needs to be able to understand the recorded ballot selection and it needs to agree with the selections made by the voter.

6 - Cryptographic E2E verifiable deals with cryptographic protocols used in cryptographic E2E verifiable (not paper-based) voting systems, requiring that they be publicly available for review for 2 years before being used in a voting system. Individuals who vote on a cryptographic E2E verifiable system will get a receipt and be able to confirm that the system correctly interpreted

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000353

their ballot selections. Voters will also be able to verify that their ballots are included in the tabulation results.

In 9.2 – Audit support requires that manufacturers identify the types of audits supported by a voting system, ensuring the system can handle audits held by election officials. The manufactures are also required to include any artifacts that the voting system produces to support the identified audits.

In 9.3 - Resilient records requires the data protection requirements under *Principle 13: Data Protection* are followed to ensure that voting system records are resilient in the presence of both intentional forms of tampering and accidental errors.

In 9.4 - Efficient audits covers requirements that ensure the system that will produce the records that allow election officials to conduct risk-limiting audits. Risk-limiting audits can detect the accuracy of a vote count within this specified margin of error.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000354

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence

9.1.1-A – Software independent

The voting system must be software independent.

1. The voting system must meet the requirements within the Paper-based System Architectures or Cryptographic E2E Verifiable System Architectures section, or both.
2. The voting system documentation must include the method used to provide software independence.

Discussion

Software independence *[Rivest06]* means that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results. All voting systems need to be software independent in order to conform to the VVSG.

There are two essential concepts behind applying software independence:

- it must be possible to audit voting systems to verify that ballots are being recorded correctly, and
- testing software is so difficult that audits of voting system correctness cannot rely on the software itself being correct.

Therefore, voting systems need to be 'software independent' so that the audits do not have to trust that the voting system's software is correct. The voting system will provide proof that the ballots have been recorded correctly, that is, voting records will be produced in ways in which their accuracy does not rely on the correctness of the voting system's software.

This is a major change from previous versions of the VVSG because previous versions permitted voting systems that are software dependent, that is, voting systems whose audits rely on the correctness of the software. One example of a software dependent voting system is the DRE, which is now non-conformant to this version of the VVSG.

There are currently two methods specified in the VVSG for achieving software independence:

- through the use of independent voter-verifiable paper records, and
- cryptographic E2E verifiable voting systems.

Paper-based and cryptographic E2E verifiable system architectures are software independent and both can be used within the same voting system. In this case where a voting system is identified as being a combination of both architectures, the system would need to be compliant with both sets of

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000355

requirements. However, a system that meets all of the paper-based requirements need not satisfy the E2E-requirements even if it incorporates E2E verifiable functionality.

Knowing the specific mechanism used to achieve software independence assists with determining if the system is truly is software independent.

The documentation should explain how any changes to the election outcome are detectable regardless of any fault or error in the voting system software. This may include how the voting systems handles a ballot after it is cast by the voter. For example, this documentation may answer the following questions:

- Is it able to print on the ballot?
- What information is printed on the ballot?
- Where is that information printed?

Related requirements can be found under: 9.1.5 – Paper records
9.1.6 – Cryptographic E2E verifiable

9.1.2 – Tamper evidence

9.1.2-A – Tamper-evident records

The voting system must produce tamper-evident records that enable detection of incorrect election outcomes, including:

1. capturing the contents of each vote at the time of each ballot's casting, and
2. recording detected errors in a tamper-evident manner.

Discussion

Tamper-evident records include CVRs, ballot images and artifacts from a cryptographic E2E verifiable voting system.

The record also ensures that identified issues and other problems cannot be lost or unintentionally modified once they are discovered.

9.1.2-B – Tamper-evident record creation

Paper records or other tamper-evident electronic records of the voter's ballot selections must be captured when each ballot is cast.

Discussion

Voter-facing scanners and other vote-capture devices produce the paper records or other tamper evident electronic records. These records can be useful artifacts for post-election audits.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000356

Applies to: Voter-facing scanners and electronic ballot markers

9.1.3 – Voter verification

9.1.3-A – Records for voter verification

The voting system must provide individual voters the opportunity to verify that the voting system correctly interpreted their ballot selections.

Discussion

- Voter-facing scanners and other vote-capture devices can be used to meet this requirement. An electronic ballot marker can print a voter's ballot selections to review before casting. An E2E verifiable system can print a receipt that allows a voter to verify their selections are tabulated and captured correctly. *Principle 7: Marked, Verified, and Cast as Intended* includes more requirements for voter verification.

Applies to: Voter-facing scanners and electronic ballot markers
Related requirements: 7.3-G – Full ballot selections review

9.1.3-B – Ballot error correction

The voting system must allow a voter to start a new voting session if they would like to correct an error found in their ballot selections.

Discussion

If, after printing their ballot, a voter decides they would like to update or change a selection before casting, the voter must be able to get a new ballot and start a new voting session to mark their ballot as they intend. A voter can contact a poll worker to spoil their current ballot, receive a new ballot, and start a new voting session.

Applies to: Paper-based system architectures
Related requirements: 7.3-F – Correcting the ballot

9.1.3-C – Voter reported errors

Voting system documentation must describe a method, either through procedural or technical means, for voters to report detected errors or incorrect results.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000357

This can include a voter alerting an election worker or pressing a button on the machine to report detected errors or incorrect results.

9.1.4 – Auditable

9.1.4-A – Auditor verification

Voting systems must generate records that would enable external auditors to verify that cast ballots were correctly tabulated.

Discussion

The voting systems themselves cannot make records available to the public. The manner and decision to make these records available is made by a state and or local jurisdiction. This requirement only ensures that the records themselves are generated and can be easily accessed without additional software or assistance from the voting system manufacturer. This requirement is meant to enable external auditors to perform their own count of the election results.

9.1.4-B – Documented procedure

The voting system manufacturer must provide a documented procedure to verify that cast ballots were correctly tabulated.

Discussion

This documentation includes procedures and technical practices that verify the results post-election and demonstrates software independence. This documentation could be used as a starting point for election officials to develop the procedures used to audit an election.

Related requirements: 9.1.1-A – Software independent

9.1.5 – Paper records

9.1.5-A – Paper record production

A paper-based voting system must produce a voter-verifiable paper record of the voter's ballot selections.

Discussion

Voting systems that use independent voter-verifiable records can satisfy the software independence requirement and achieve conformance to the VVSG.

Related requirements: 3.3-C – Bar and other codes

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000358

3.3-D – Ballot selection codes
5.1-E – Reading paper ballots
6.1-A – Preserving privacy for voters
6.2-A – Voter independence
9.1.5-C – Paper record intelligibility
9.1.5-D – Matching selections

9.1.5-B – Paper record retention

A paper-based voting system must retain a paper record of the voter's ballot selections.

9.1.5-C – Paper record intelligibility

The recorded ballot selections must be presented in a human-readable format that is understandable by the voter.

Discussion

The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.

Applies to: Paper-based system architectures

9.1.5-D – Matching selections

All representations of a voter's ballot selections produced by the voting system must agree with the selections made by the voter.

Applies to: Paper-based system architectures

9.1.5-E – Paper record transparency and interoperability

All barcode representations of a voter's ballot selections must use an open and interoperable format.

Related requirements: 3.3-C – Bar and other codes
3.3-D – Ballot selection codes

9.1.5-F – Unique identifier

A paper-based voting system must be capable of adding a unique identifier after a voter casts their ballot.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000359

Although not all jurisdictions may use this feature, voting systems are required to have the capability to add a unique identifier to ballots.

Applies to:	Paper-based system architectures
Related requirements:	1.1.5-G – Record audit information 9.4-A – Risk-limiting audit 9.4-B – Random numbers supporting audit processes 9.1.1-A – Software independent

9.1.5-G – Preserving software independence

After a voter verifies their selections on a voted ballot and submits the ballot for casting, a paper-based voting system must not be capable of making an undetectable change to the paper record.

Discussion

After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To preserve software independence the voting system should not be able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead the voting system should only be able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color.

This printing process should be preserved regardless of software or hardware updates.

Related requirements:	9.1.1-A – Software independent

9.1.6 – Cryptographic E2E verifiable

9.1.6-A– Verified cryptographic protocol

The E2E cryptographic protocol used by the cryptographic E2E verifiable voting system must be evaluated and approved through a public process established by the EAC.

Discussion

Due to the lack of E2E verifiable voting systems available within the current market, there are no verified E2E cryptographic protocols. A standard public process for approval of the E2E cryptographic protocols will need to be established outside of the VVSG. Once this process is established, the VVSG requirements can point to the approved/verified cryptographic protocols as acceptable for use within an E2E verifiable voting system.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000360

9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation

A cryptographic E2E verifiable voting system must undergo an independent evaluation to verify it correctly and securely implements an approved E2E cryptographic protocol.

Discussion

An independent evaluation can be performed by any entity outside of the voting system manufacturer. Example best practices include using guidance from the *FIPS 140 series [NIST01, NIST19a], NIST SP 800-133 Revision 2, Recommendation for Cryptographic Key Generation [NIST20f],* or *NIST SP 800-175B*, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms [NIST20g].* The independent evaluation and cryptographic engineering best practices used can be documented and submitted.

Lessons learned from the analysis of the source code of the Swiss Post system shows the value in making this code available for public review. See "How not to prove your election outcome" *[Lewis19b],* and "Ceci n'est pas une preuve" *[Lewis19a].*

9.1.6-C – Cryptographic ballot selection verification by voter

A cryptographic E2E verifiable voting system must:

1. be capable of providing evidence that an individual voter can use to confirm that the voting system correctly interpreted their ballot selections, while in the polling place; and
2. provide evidence such that if there is an error or flaw in the interpretation of the voters' selections, the evidence can be used for detection of the error or flaw.

Discussion

This requirement addresses cast-as-intended verification, which is one of the principal components necessary to achieve end-to-end- verifiability *[Benaloh14].*

Interpretation is the process by which the voting system converts the voter's contest option selections into the format used to store these selections. Therefore, this evidence must sufficiently prove the representation of the voter's contest option selections in digital form matches the voter selections as provided to the system.

Giving voters the opportunity to verify the voting system stored their ballot choices correctly is a fundamental building block in an end-to-end verifiable voting system.

See "End-to-end verifiability" *[Benaloh14]* and "Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability" *[Kulyk18]* for more information on the various implementations of this technique.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000361

Related requirements: 6.2-A – Voter independence
7.3-G – Full ballot selections review
9.1.6-E – Ballot receipt
10.2.4-A – Voting information in receipts

9.1.6-D – Methods for cryptographic ballot selection verification

1. A cryptographic E2E verifiable voting system documentation must include: the method for the voter to use the evidence provided for ballot selection verification to verify the correct interpretation of their ballot; and
2. a list of known verification tools, their supplier, and how the verification tools are used.

Discussion

Voter intent verification often relies on external verification tools to assist voters in the verification step(s). These can be external verifiers, which is either a second device, a website of a trusted institution, or software running inside the polling location. The manufacturer must provide documentation explaining the verification options available to voters. If the jurisdiction is expected to provide the verification tool or service, this must also be documented.

Related requirements: 9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-E – Ballot receipt

A cryptographic E2E verifiable voting system must provide a voter with a receipt that allows them to verify that their ballot has been correctly recorded and tallied by the system. These receipts

1. must not display any ballot selections made by the voter;
2. must not enable the voter to prove their selections on the cast ballot to others;
3. must be represented in a publicly documented format;
4. may contain a unique identifier; and
5. are accessible, verifiable, and preserve voter-privacy.

Discussion

This evidence should fail to confirm a voter's ballot has been correctly recorded and tallied by the system if the ballot has been removed, tampered with, or its selections altered, added to, or removed.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000362

Related requirements: 6.1-A – Preserving privacy for voters
6.2-A – Voter independence
7.3-G – Full ballot selections review
8.3-A – Usability tests with voters
10.2.4-A – Voting information in receipts

9.1.6-F – Disputes involving ballot receipts

The cryptographic E2E verifiable voting system documentation must provide procedures for collecting, investigating, and adjudicating disputes from voters based on the contents of their ballot receipts.

Discussion

This documentation will include a process to address the scenario where a voter attempts to verify with their ballot receipt and believes there is a problem with their ballot receipt

Related requirements: 9.1.6-E – Ballot receipt

9.1.6-G – Evidence export

A cryptographic E2E verifiable voting system must:

1. be capable of exporting all evidence supporting ballot tabulation verification, and
2. provide the export in an open and consumable format.

Discussion

Most recorded-as-cast verification approaches require the public posting of the evidence at some point after all ballots have been aggregated and tallied. As required in the previous requirement, the evidence must not reveal how voters voted.

9.1.6-H– Mandatory ballot availability

A cryptographic E2E verifiable voting system must be capable of exporting all encoded ballots for public posting.

Discussion

The public posting does not have to be provided by the voting system, but the voting system must provide the evidence such that it can be published, and the verification process made accessible to voters. The public posting of these exported encoded ballots is performed by election officials and is an essential part of the E2E verifiable process. It allows the public to verify the election results.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000363

9.1.6-I – Verification of encoded votes documentation

A cryptographic E2E verifiable voting system documentation must include:

1. the expected method by which voters will perform the ballot tabulation verification, and
2. how this method provides voters with the opportunity to verify that their ballots are included within the tabulation results.

Discussion

For example, a common method is to publish the evidence to a public bulletin board. The manufacturer should document this method or its alternative. The bulletin board, itself, might not be included in the scope of the voting system but the voting system must provide an export of the evidence to be published on the bulletin board.

9.1.6-J – Verifier reference implementation

A cryptographic E2E verifiable voting system documentation must include:

1. a free publicly available reference implementation of a tool which can be used:
    a. to verify evidence provided to a voter to prove that their ballot choices were correctly interpreted, and
    b. to verify the evidence reported for voters to perform ballot tabulation verification;
2. the build instructions for the reference implementation, along with the tool.

Discussion

For the system to support the cast-as-intended property of end-to-end verifiable systems there must be at least one tool available to voters to verify that their ballot selections have been correctly interpreted. Additionally, for a cryptographic E2E system be software independent, the voters need to have choices about what software use and trust when performing verification. By providing an open source reference implementation may facilitate development of third-party verification tools.

Related requirements: 9.1.6-C – Cryptographic ballot selection verification by voter

9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

A cryptographic E2E verifiable voting system tabulation process must preserve the privacy of every voter and provide a method for public verification.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000364

To be publicly verifiable, the approach provides a means for any auditor or observer to verify the correct decryption and tabulation of the votes (not necessarily in that order) using cryptographic proofs that are generated by the process.

Related requirements: 6.1-A – Preserving privacy for voters

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000365

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Audit support documentation

The voting system documentation must specify the types of audits the voting system supports and the artifacts that the voting system provides to support those audits.

Discussion

Ballots, CVRs, and ballot images are examples of artifacts that can support a post-election audit.

Related requirements: 1.1.9-A – Post-election reports
3.1.3-D – Audit procedures

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records

All voting systems must meet the requirements listed under Guidelines *13.1* and *13.2* that are related to protecting audit records.

Discussion

CVRs and ballot images need sufficient data protection because they are needed for audits.

Related requirements: 13.1.2-A – Integrity protection for election records
13.2-A – Signing stored election records
13.2-B – Verification of election records

AMERICAN OVERSIGHT

9.4 - The voting system supports efficient audits.

9.4-A – Risk-limiting audit

A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit.

Discussion

Voting systems contain information which enables election officials to conduct risk-limiting audits. For example, batch subtotal reporting by the voting system, may make the process of ballot sampling more efficient.

An evidence-based election requires convenient access to ballot sheets, ballot sheet images, and cast vote records for efficient and trustworthy public tabulation audits. Vendors should demonstrate how an election system provides all the information necessary for an independent Risk-Limiting Audit (RLA).

Some example features/paper records that may be produced to support risk-limiting audits include the following:

- the ability to associate electronic cast vote records (CVRs) with corresponding paper records while also preserving ballot secrecy;
- the ability to export of CVRs in an open and interoperable format;
- the ability to create a ballot manifest that allows users to identify the physical location of ballots (e.g., scanner name or number, batch number, and ballot sequence number); and
- supporting multi-sheet ballots, including association of each sheet with its corresponding CVR.

Related requirements:
4.1-C – Exchange of cast vote records (CVRs)
9.1.5 – Paper records
9.2-A – Audit support documentation
9.4-C – Unique ballot identifiers
9.4-D – Multipage ballots

9.4-B – Random numbers supporting audit processes

Voting systems that generate or rely on random or pseudo-random numbers for auditing purposes must document the method used to obtain the numbers and how the random numbers are used within the voting system.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000367

Various systems used to implement software independence require random numbers, whether for ballot selection for audits.

This documentation should specify:

- how random numbers are generated, and
- what any random numbers are used for.

One common use for random numbers is to create unique identifiers associated with ballots to assist in supporting audits.

The method for generating the pseudo-random numbers should meet the requirement *10.2.2-E Randomly generated identifiers.*

For additional information, see *NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a].*

Related requirements: 9.4-C – Unique ballot identifiers
10.2.2-E – Randomly generated identifiers

9.4-C – Unique ballot identifiers

The voting system must enable election auditors to uniquely address individual ballots.

Discussion

This capability is needed to support RLAs. Although the voting system has this capability, this does not require jurisdictions to use this feature if it conflicts with state laws. In order to conduct a ballot-comparison risk-limiting audit, paper ballot records must either be stored in the order in which they were scanned or contain a unique ballot identifier. A unique ballot identifier is a unique ID that provides information about the device it was scanned on and the batch in which it is stored. One example of a unique ballot identifier is: scanner ID, batch ID, and ballot card number. The unique ballot identifier must not tie a ballot to an individual voter

9.4-D – Multipage ballots

The voting system must be able to account for multipage ballots.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000368

Principle 10
Ballot Secrecy

The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000369

Principle 10
Ballot Secrecy

The voting system protects the secrecy of voters' ballot selections.

The requirements for *Principle 10* include ensuring ballot secrecy and ensuring that nothing is produced that would associate the voter's identity with their votes. A related topic, *Principle 6: Voter Privacy*, covers voter privacy during voting.

10.1 - Use of voter information covers the requirement that ballot secrecy is maintained throughout the voting process.

The sections in ***Guideline 10.2*** cover:

1 – Voter associations requires that there be no direct or indirect association between the voter's identity and their ballot, with the exception of certain instances when used in cryptographic end-to-end (E2E) verifiable voting systems. It covers how election workers must select the indirect association option and how these ballots are to be stored separately from cast ballots. It also requires encryption of ballots not yet cast that contain an indirect association.

2 – Identification in vote records covers the use of identifiers for tying cast vote records (CVRs) and ballot images to paper ballots and the need for them to be distinct from identifiers used for indirect associations. The voting system cannot allow for any information that could be used to determine the order in which votes are cast or include any information identifying a voter. Aggregate and final totals must also not allow identification of a voter. The goal is to ensure that a voter cannot be identified from the format of the ballot or method of voting. Best practices in polling places are also critical to ensuring that there are enough BMD-printed ballots to preserve ballot secrecy.

3 – Access to cast vote records (CVRs) covers the need to limit information about and access to the storage location for CVRs, ballot images and ballot selections. Any such access needs to be authorized and logged.

4 – Voter information in other devices and artifacts requires that receipts produced by a voting system cannot contain voter information and must not violate ballot secrecy. Logs cannot contain individual or aggregate selections, nor can activation devices create or retain information that can be used to identify a voter's ballot. It should not be possible for any part of the voting system to be used to violate ballot secrecy, including in the absence of a ballot

AMERICAN OVERSIGHT

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System use of voter information

The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter.

Discussion

Examples include first name, last name, address, driver's license, and voter registration number and other personally identifiable information (PII). This requirement applies to the voting system itself, as the voting system cannot prevent a voter from self-identifying within write-in fields or other areas of the ballot.

Related requirements: 11.1-B – Voter information in log files

10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

10.2.1 – Voter associations

10.2.1-A – Direct voter associations

The voting system must not create or store direct associations between a voter's identity and their ballot.

Discussion

A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number, voter identification number, or driver's license number. (This is not an exhaustive list of direct voter association examples.)

10.2.1-B – Indirect voter associations

Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.

Discussion

AMERICAN OVERSIGHT

Certain channels of voting require indirect associations so that ineligible ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. The most common example of indirect association would be a randomly generated number. Best practice would ensure that indirect voter associations are only available to authorized election personnel.

This requirement only applies to paperless voting systems that also meet the requirements under *Guideline 9.1*, which states that the voting system must be software independent. During the writing of these requirements, cryptographic E2E verifiable voting systems are a potential paperless and software independent system that could be applicable for this requirement.

Applies to: Cryptographic E2E verifiable voting system architectures

10.2.1-C – Use of indirect voter associations

The voting system must only use indirect voter associations when the option is selected at the beginning of a voting session for situations when a voter needs to fill out a ballot before their eligibility is determined.

Discussion

Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. These types of ballots are often considered provisional or recallable ballots.

Applies to: Cryptographic E2E verifiable voting system

10.2.1-D – Isolated storage location

Ballots that are not cast and contain an indirect association must be separated from cast ballots.

Discussion

Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.

Applies to: Cryptographic E2E verifiable voting architectures

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000372

10.2.1-E – Removal of indirect voter associations

The voting system must be capable of removing the indirect voter association between a ballot and a voter once that voter is determined to be eligible.

Discussion

Provisional or recallable ballots may require indirect associations so that ballots can be removed before casting. After a voter's eligibility is determined the indirect voter association can be removed and the ballot can be added to collection of cast ballots. In the case of electronic E2E systems, whatever data record provides this association must be removed from the system.

Ballots with indirect associations are not considered cast until the association is removed. Best practice would ensure that indirect voter associations are only available to authorized election personnel.

Applies to: Cryptographic E2E verifiable voting architectures

10.2.1-F – Confidentiality for ballots with indirect voter associations

The voting system must only be capable of decrypting a ballot after any indirect voter association to it has been removed.

Discussion

Encryption of the ballot preserves the confidentiality of the voter's ballot selections while the ballot is tied to an indirect association to the voter. The indirect voter association is not encrypted with the ballot.

The voting system must not be capable of decrypting a ballot that still has an indirect association to a voter. A possible approach to implement this is by requiring that a decryption key (or set of keys) be entered to decrypt ballots but disallowing input until after all indirect associations have been removed. If the key is present on the system at the same time as indirect associations, it may be possible for malicious software to decrypt ballots and associate selections with voters.

Applies to: Cryptographic E2E verifiable voting architectures

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000373

10.2.2 – Identification in vote records

10.2.2-A – Identifiers used for audits

Identifiers used for tying a cast vote record (CVR) and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.

Discussion

For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.

Related requirements: 9.1.5-F – Unique identifier

10.2.2-B – No voter record order information

The voting system must not contain data or metadata associated with the CVR and ballot image files that can be used to determine the order in which ballots votes are cast.

Discussion

No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent. Otherwise, metadata can be useful for verification. For instance, date of creation of record in the voter-facing device might reveal the order of voting. Most other metadata won't be a problem.

10.2.2-C – Identifying information in voter record file names

CVR and ballot image file names must not include any information identifying a voter.

Discussion

This helps to ensure that information that could accidently be used to reference a voter is not used within a file name.

10.2.2-D – Aggregating and ordering

Aggregated and final totals:

1. must not contain voter identifying information, and
2. must not be able to recreate the order in which the ballots were cast.

Discussion

Voter identifying information includes social security number, voter identification number, or driver's license number.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000374

10.2.2-E – Randomly generated identifiers

Randomly generated identifiers used for audits must use random bit generators specified in the latest revision of *NIST SP 800-90* series on random bit generators.

Discussion

This requirement is important to ensure the use of a cryptographically secure pseudo-random number generator (CSPRNG) and also to ensure any random numbers, such as unique identifiers on a ballot, cannot be used to recreate the order in which a ballot was cast. Recreating the order of cast ballots can cause ballot secrecy issues if a voter's ballot can be identified.

To ensure voting system vendors are following the random number generation recommendations in the 800-90 series, they will need to submit to the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) for conformance testing.

For additional information, see *NIST SP 800-90A Rev 1*, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a]* and *NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation [NIST18a].*

Related requirements: 9.4-B – Random numbers supporting audit processes
10.2.2-D – Aggregating and ordering

10.2.3 – Access to cast vote records (CVR)

10.2.3-A – Restrict access to records of voter intent

The voting system must require administrator-level authorization to access the directory or storage location of CVRs, ballot images, and ballot selections.

Discussion

Cast vote records, ballot images, and ballot selections should be subject to special restrictions on access. Permissions to access these storage locations are limited only to those users who need to access the location. This may be especially essential during voting to protect ballot secrecy and avoid any exposure of results until polls are closed.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators
11.4-A – Least privilege for access policies
11.4-B – Separation of duties

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000375

10.2.3-B – Digital voter record access log

The voting system must log all access to the directory or storage location for CVRs, ballot images, and ballot selections in addition to logging access to all actions occurring within the system.

Discussion

This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged.

This requirement does not apply when the CVR, ballot images, and ballot selections are stored on removable media and removed from the vote-capture device.

Related requirements: 11.1-A – Logging activities and resource access

10.2.4 – Voter information in other devices and artifacts

10.2.4-A – Voting information in receipts

Receipts produced by cryptographic E2E verifiable voting systems must not contain voter information.

Discussion

The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

10.2.4-B – Logging of ballot selections

Logs and other portions of the audit trail must not contain individual or aggregate ballot selections.

Discussion

The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and possibly even to the public, if election officials so desire. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000376

10.2.4-C – Activation device records

Ballot activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system.

Discussion

Information such as the time the voter arrived at the polls or the specific vote-capture device used by the voter may be used to link a voter with their specific ballot and violates the principle of ballot secrecy.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000377

Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties.

11.5 - Logical access to voting system assets are revoked when no longer required.

AMERICAN OVERSIGHT

Principle 11
Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

The requirements for *Principle 11* cover how the voting system secures and limits access to only those who are authorized.

11.1 – Access privileges, accounts, activities and authorizations are logged, monitored, and reviewed and modified as needed ensures there are records in case there are errors or incidents that need to be accounted for. The system also prevents logging any voter ID information and prevents the logging capability from becoming disabled or the log entries from being modified. The system provides administrators access to logs, allowing for continuous monitoring and periodic review.

The sections in ***Guideline 11.2*** cover:

1 – Authorized access ensures that only authorized users can access the voting system. All voting systems will have an administrator role and only administrators can create or modify authorized users, configure permissions, and create or assign groups or roles. Control mechanisms distinguish at least four voting stages: Pre-voting, Activated, Suspended, and Post-Voting. Differentiating theses stages helps limit access to the voting system to only those individuals strictly necessary at any given time.

2 – Role-based access control covers to the requirement that voting systems that implement role-based access control support the ANSI Core Role Based Access Control (RBAC) recommendations. Systems that implement RBAC define groups or roles. Voting systems use the groups and stages described above to assign minimum permissions to authorized users, limiting each person's access within the system.

The sections in ***Guideline 11.3*** cover:

1 – Access control mechanisms either permit authorized access or prevent unauthorized access to the voting system. This includes the capability of using multi-factor authentication to verify a user's authorized access to perform critical operations. It also authenticates the administrator with a multi-factor authentication mechanism. Multi-factor authentication provides additional security beyond the use of a single password.

2 – User Authentication Credentials covers the requirement that only the administrator can specify and enforce password strength, histories, and expiration, when that authentication method is used. The system will also compare all passwords against a manufacturer-specified

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000379

list of well-known weak words and will ensure that the username is not used in the password. The voting system will securely store passwords and other authentication credentials (such as multi-factor authentication codes).

11.4 – Default access control policies enforce the principles of least privilege, minimizing access within the system to only what is strictly necessary, and separation of duties, narrowing roles so that access isn't granted too broadly for any group of users.

11.5 – Logical access restrictions. The voting system only allows users access within the time period specified by the administrator. The system locks out roles or individuals after a specified number of consecutive failed attempts, and it allows only an administrator to define the lockout duration. This can help prevent unauthorized use if a system is left unattended.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000380

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.1-A – Logging activities and resource access

The voting system must log any access to, and activities performed on, the voting system, including:

1. timestamps for all log entries;
2. all failed and successful attempts to access the voting system; and
3. all events which change the access control system including policies, privileges, accounts, users, groups or roles, and authentication methods.

Discussion

In the event of an error or incident, the user access log can assist in narrowing down the reason for the incident or error.

- Timestamped log entries will allow for easy auditing and review of access to the voting system.
- Access control logging supports accountability of actions by identifying and authenticating users.
- Groups are a collection of users that are assigned a specific set of permissions. Roles are an identity that is given specific permissions and can be assigned to a user. Any changes to the permissions assigned to groups and roles should be logged to identify updates to a user's privileges.

11.1-B – Voter information in log files

The voting system must not log any voter identifying information.

Discussion

The logging and storing of voter identifying information after a ballot is cast potentially violates voter privacy and ballot secrecy. Examples of voter identifying information include first name, last name, address, driver's license, and voter registration number.

Related requirements: 10.1-A – System use of voter information
10.2.4-B – Logging of ballot selections

11.1-C – Preserving log integrity

The voting system must prevent:

1. the logging capability from being disabled;

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000381

2. the log entries from being modified in an undetectable manner; and
3. The deletion of logs; with the exception of log rotation.

Discussion

This requirement promotes the integrity of the information logged by ensuring all activities are logged. Additionally, it prevents these abilities from being an option within the user interface.

This requirement promotes the integrity of the information logged by ensuring all activities are not modifiable.

The removal of logs is only appropriate for log rotation, which is when the stored logs are rotated out to create more space for continuous logging. The voting system should be capable of rotating the event log data to manage log file growth. Log file rotation may involve regular (e.g., hourly, nightly, or weekly) moving of an existing log file to some other file name and/or location and starting fresh with an empty log file. Preserved log files may be compressed to save storage space.

11.1-D – On-demand access to logs

The voting system must provide administrators access to logs on demand, allowing for continuous monitoring and periodic review.

Discussion

Enabling administrators to export and review the logs is a useful feature. Continuous monitoring and review of access control logs gives the administrator the opportunity to analyze and make changes to permissions and privileges, and quickly identify issues.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000382

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access

11.2.1-A – Ensuring authorized access

The voting system must allow only authorized users to access the voting system.

Discussion

Authorized users include voters, election officials, and election workers.

11.2.1-B – Modifying authorized user lists

The voting system must allow only an administrator to create or modify the list of authorized users.

Discussion

This requirement assists with ensuring only authorized users are given access to the voting system.

11.2.1-C – Access control by voting stage

The voting system access control mechanisms must distinguish at least the following voting stages from Table 11-1:

1. Pre-voting
2. Activated
3. Suspended
4. Post-voting

Table 11-1 – Voting stage descriptions

Stage	Description
Pre-voting	Loading, and configuring device software, maintenance, loading election-specific files, preparing for election day usage
Activated	Activating the ballot, printing, casting, spoiling the ballot
Suspended	Occurring when an election official suspends voting

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000383

Post-voting	Closing polls, tabulating votes, printing records

Discussion

The groups or roles in 11.2-H (Table 11- 2) will be given specific permissions which can be affected by the voting stage (Table 11-1).

11.2.1-D – Access control configuration

The voting system must allow only an administrator to configure the permissions and functionality for each identity, group or role, or process to include account and group or role creation, modification, disablement, and deletion.

Discussion

For vote-capture devices, it is possible for each group or role to have (or not have) permissions for every voting stage. Additionally, the permissions that a group or role has for a voting stage can be restricted to certain functions. Table 3 shows an example matrix of group/role to system to voting state access rights; the table is not meant to include all activities. This requirement extends *[VVSG2005] I.7.2.1.1-a* by allowing configuration flexibility for permissions and functionality for each identity or group/role.

Privileged accounts include any accounts within the operating system, voting device software, or other third-party software with elevated privileges such as administrator, root, and maintenance accounts. This requirement extends *[VVSG2005] I.7.2.1.2* by allowing the creation and disabling of privileged accounts.

An administrator is the only user authorized to make major changes within a voting system. Administrators are given this group or role to ensure all other users have proper access to the information necessary to perform their duties.

11.2.1-E – Administrator modified permissions

The voting system must allow only an administrator to create or modify permissions assigned to specific groups or roles.

Discussion

The administrator's authority to create or modify permissions restricts users from gaining unauthorized permissions.

11.2.1-F – Authorized assigning groups or roles

The voting system must allow only an administrator to create or assign the groups or roles.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000384

Discussion

Table 2 is a list of groups or roles that need to be included within the voting system.

Related requirements: 11.2.2-B – Minimum groups or roles

11.2.2 – Role-based access control

11.2.2-A – Role-based access control standard

Voting systems that implement role-based access control must support the recommendations for Core Role Based Access Control (RBAC) in the *ANSI INCITS 359-2004 American National Standard for Information Technology – Role Based Access Control [ANSI04]* document.

Discussion

This requirement extends *[VVSG2005] I. 7.2.1.1-a* by requiring role-based methods to follow *ANSI INCITS 359-2004 [ANSI04].*

11.2.2-B – Minimum groups or roles

At minimum, voting systems that implement RBAC must define groups or roles with the role descriptions within Table 11-2.

Table 11-2 – Minimum voting system groups or roles for RBAC

Group or role	Role description
Administrator	Can update and configure the voting devices and troubleshoots system problems.
Voter	A restricted process in the vote-capture device. It allows the vote-capture device to enter the activated state for voting activities.
Election Worker	Has the ability to open the polls, close the polls, recover from errors, and generate reports; Checks in voters and activates the ballot style; Loads ballot definition files.

Discussion

Table 11-2 is a baseline list of groups or roles to be included in the voting system.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000385

11.2.2-C – Minimum group or role permissions

At minimum, the voting system must use the groups or roles from *Table 11-2 – Minimum voting system groups or roles for RBAC* and the voting stages from *Table 11-1 – Voting stage descriptions*, to assign the minimum permissions in *Table 11-3*.

Discussion

Table 11-3 – Minimum permissions for each group or role defines the minimum functions according to user, voting stage, and system. Other capabilities can be defined as needed by jurisdiction.

Table 11-3 - Minimum permissions for each group or role

Group/Role	System	Pre-Voting	Activated	Suspended	Post-Voting
Administrator	EMS	Full Access	Full Access	Full Access	Full Access
	Electronic BMD	Full Access	Full Access	Full Access	Full Access
	Voter-Facing Scanner	Full Access	Full Access	Full Access	Full Access
Voter	EMS	---	---	---	---
	Electronic BMD	---	Vote and cast ballots	---	---
	Voter-Facing Scanner	---	Ballot Submission	---	---
Election Worker	EMS	Define and load election programming	---	---	Reconcile provisional or challenged ballots, write-ins, generate reports
	Electronic BMD	Open polls, L&A	Close or suspend polls, Recover from errors, Activate ballot and cancel unvoted ballots	Exit suspended state	Generate reports

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000386

	Voter-Facing Scanner	Open polls, L&A	Recover from errors	Exit suspended state	Generate reports

11.2.2-D – Applying permissions

The voting system must be capable of applying assigned groups or roles and permissions to authorized users.

Discussion

Once the user is assigned a group or role, the voting system needs to be capable of making the necessary changes to the user's permissions. The permissions are changed based on the assigned group or role.

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanisms

11.3.1-A – Access control mechanism application

The voting system must use access control mechanisms to permit authorized access or prevent unauthorized access to the voting system.

Discussion

Access controls support the following concepts:

- limiting the actions of users, groups or roles, and processes to those that are authorized;
- limiting entities to the functions for which they are authorized;
- limiting entities to the data for which they are authorized; and
- accountability of actions by identifying and authenticating users.

Most modern operating systems natively provide configurable access control mechanisms that the voting system application can use.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000387

11.3.1-B – Multi-factor authentication for critical operations

At a minimum, the voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. runtime software updates to the certified voting system;
2. aggregation and tabulation;
3. enabling network functions;
4. changing device states, including opening and closing the polls;
5. deleting or modifying the CVRs and ballot images; and
6. modifying authentication mechanisms.

Discussion

NIST SP 800-63-3, Digital Identity Guidelines [NIST17c] provides additional information useful in meeting this requirement. *NIST SP 800-63-3* defines multi-factor authentication (MFA) as follows:

"An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

Multifactor authenticators include, but are not limited to the following:

- Username & password
- Smartcard (for example, voter access card)
- iButton
- Biometric authentication (for example, fingerprint)

Multi-factor authenticators can be tested for usability to ensure an appropriate balance of security, usability, and functionality. A significant impact to usability may require revision of the multi-factor authenticator implementation.

Related requirements: 8.4-A – Usability testing with election workers

11.3.1-C – Multi-factor authentication for administrators

The voting system must authenticate the administrator with a multi-factor authentication mechanism.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000388

Discussion

This requirement extends *[VVSG2005] I.7.2.1.2-e* by requiring multi-factor authentication for the voting system administrator group or role.

11.3.2 – User authentication credentials

11.3.2-A – Username and password management

If the voting system uses a username and password authentication method, the voting system must allow only the administrator to enforce password strength, histories, and expiration.

Discussion

This requirement extends *[VVSG2005] I.7.2.1.2-e* by requiring strong passwords, password histories, and password expiration.

11.3.2-B – Password complexity

The voting system must, at minimum, meet the password complexity requirements within the latest version of *NIST SP 800-63B Digital Identity Guidelines* standards.

Discussion

NIST SP 800-63B [NIST17d] does not specify any additional password complexity requirements besides password length. At the time of this writing, the only recommended password complexity requirement is a minimum password length of 8 characters. *NIST SP 800-63B* also recommends that if a password is provided to the user it may be 6 characters and all numeric. NIST's password complexity recommendations are meant to make it easier for users to memorize their passwords, while decreasing user frustration.

11.3.2-C – Secure storage of authentication data

The voting system must store authentication data in a way that ensures confidentiality and integrity are preserved.

Discussion

Ensuring the confidentiality of stored authentication data (such as passwords) may involve the use of cryptography. The best practice at the time of this writing is to store a salted, one-way hash of passwords. Additional guidance for protecting authentication data can be found in *NIST SP 800-63B, Digital Identity Guidelines [NIST17d].*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000389

11.3.2-D – Password disallow list

The voting system must compare all passwords against a manufacturer-specified list of well-known weak passwords and disallow the use of these weak passwords.

Discussion

Examples of common weak passwords include 0000, 1111, 1234.

11.3.2-E – Usernames within passwords

The voting system must ensure that the username is not used in the password.

Discussion

This requirement extends by restricting the use of usernames and related information in passwords.

11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties.

11.4-A – Least privilege for access policies

By default, the voting system must implement the principle of least privilege including denying access to functions and data unless explicitly permitted.

Discussion

This requirement extends *[VVSG2005] I.7.2.1.2-a* by requiring explicit authorization of subjects based on access control policies.

At the time of this writing, *NIST SP 800-12 [NIST17e]* defines "least privilege" as "the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function."

Network access will also follow the principle of least privilege to ensure that devices only receive as much access as is necessary to perform the desired function.

11.4-B – Separation of duties

Voting system documentation must include suggested practices for dispersing critical operations across multiple groups or roles.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000390

Guidance for implementing separation of duties within the voting system is imperative to implement the separation of duties principle. Separation of duties is meant to divide user functions and roles so that there is no conflict of interest.

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5-A – Session time limits

The voting system must enable an administrator the ability to do the following:

1. set the maximum time limit for a user's session, and
2. set the maximum time limit for user inactivity.

Discussion

NIST SP 800-63B [NIST17d] recommends a max session time of 12 hours regardless of inactivity and a max inactivity time of 30 minutes. Elections consist of temporary employees and user access may only be required during an election. A user's access may expire and terminate automatically at the end of an election.

Related requirements: 11.5-B – Reauthentication

11.5-B – Reauthentication

The voting system must require reauthentication of an authorized user after the administrator-specified time limit for the user's session or for user inactivity.

Discussion

After authentication, a user's access to a voting system will time-out after a specified period of time. This will avoid unauthorized access to the voting system by unauthorized users. Once a user's access has timed-out, the user will have to re-authenticate to continue using the voting system.

For voters, session times are specified under requirement *7.2-O – Inactivity alerts*.

For more information, see *NIST SP 800-63B [NIST17d]*.

Related requirements: 7.2-O – Inactivity alerts
11.5-A – Session time limits

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000391

11.5-C – Account lockout

The voting system must lockout roles or individuals after an administrator-specified number of consecutive failed authentications attempts.

Discussion

This requirement prevents certain classes of password guessing attacks. This requirement can be implemented using a technique such as exponential backoff. *NIST SP800-63B* recommends allowing 5-10 attempts before starting exponential backoff. Exponential backoff requires that after each unsuccessful authentication attempt, the time period before another authentication attempt can be made grows exponentially. For instance:

- The wait after 1 unsuccessful authentication attempt is 0 seconds
- The wait after 2 unsuccessful attempts is 2 seconds
- The wait after 3 unsuccessful attempts is 4 seconds, and so on

11.5-D – Lockout time duration

The voting system must allow only an administrator to define the lockout duration.

Discussion

This requirement extends *[VVSG2005] I.7.2.1.2* by allowing the administrator flexibility in configuring the account lockout policy. The lockout policy should not lockout voters.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000392

Principle 12
Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000393

Principle 12
Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

The requirements for *Principle 12* cover the mechanisms that will protect the physical security of the voting system.

12.1 – Mechanisms to detect unauthorized physical access deals with the requirement that unauthorized physical access leave physical evidence, including access to containers holding voting system records. Devices need to produce an alert if access to a restricted voting device component is detected or if a connected component is physically disconnected during the activated state. The voting system needs to log when a device or component is connected or disconnected during an activated state and log the status of physical access points when the system is booted.

Locks installed in voting devices for security must be tested and be designed with countermeasures to indicate unauthorized attempts have been made to gain access to the voting device. Locking systems will be flexible enough to support different keying schemes. Backup power for power-reliant countermeasures is also required.

12.2 – Physical ports and access points essential to voting operations covers the requirement that voting devices have or expose only those physical ports and access points that are essential to voting operation, testing, and auditing. If a physical connection between components is broken during an activated or suspended state, the affected voting device port will be automatically disabled. The voting system will restrict physical access to any port that accommodates removable media, except for ports that activate a voting session. Devices need to allow authorized administrators to put physical ports into a disabled state. An event entry log that identifies the name of the affected device will be generated when physical ports are enable or disabled.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000394

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1-A – Unauthorized physical access

Any unauthorized physical access to voting systems must leave physical evidence that an unauthorized event has taken place.

Discussion

Access points such as covers and panels need to be secured by locks or other mechanisms that leave physical evidence in case of tampering or unauthorized access. Manufacturers can provide for and recommend a combination of procedures and physical measures that allow election officials to differentiate authorized from unauthorized access during all modes of operation, such as a system that relies on tamper evident tape, seals, or tags coded with consecutive serial numbers. Other systems might use seals incorporating radio frequency identification devices with physically unclonable functions or other technology in the future.

This requirement extends *[VVSG2005] I.7.3.1* by requiring that any tampering with a device leave physical evidence. *[VVSG2005] I.7.3.1* states that any tampering should be detectable using manufacturer-specified procedures and measures.

12.1-B – Unauthorized physical access alert

Voter-facing scanners and electronic BMDs must produce an alert if access to a restricted voting device component is detected during the activated voting stage.

Discussion

This alert is meant to call attention to election workers in the polling place.

More information about the activated stage is defined in *Table 11-1.*

Related requirements: 11.2.1-C – Access control by voting stage

12.1-C – Disconnecting a physical device

Voter-facing scanners and electronic BMDs must produce an alert if a connected component is physically disconnected during the activated voting stage.

Discussion

An alert can be provided in the form of an alarm to provide an audible and/or visual alert. Examples of connected components include printers, removable storage devices, and mechanisms used for

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000395

networking. If a token is necessary for normal operation, such as a memory card or other device granting a voter access to the voting system, it is not necessary to trigger the alert.

More information on the activated stage is defined in *Table 11-1*.

12.1-D – Logging of physical connections and disconnections

The voting system must log when a voter-facing scanner, electronic BMD, or other component is connected or disconnected during the activated voting stage.

Discussion

Logging of the devices is vital for determining cause and providing incident information if a physical security event occurs.

Related requirements: 11.2.1-C – Access control by voting stage
15.1-D – Logging event types

12.1-E – Secure containers

Unauthorized physical access to a container that stores or transports voting system records must result in physical evidence that an unauthorized event has taken place.

Discussion

The goal is to ensure that election workers or observers would easily notice if someone has tampered with the container. This requirement can be achieved through locks or seals as a part of tamper evidence and tamper resistance countermeasures described by the use procedures and supplied by the manufacturer.

Additionally, to support the requirements in *Principle 9-Auditable*, containers which hold either paper or electronic voting system records needed for audits need to be secure against physical access. An example of a physical container includes ballot boxes integrated and sold as part of the voting system.

Applies to: Voter-facing scanners, BMDs

12.1-F – Secure locking systems

If the voting system uses locks it must support locking systems for securing voting devices that are flexible enough to support different keying schemes, including a scheme that can make use of keys that are unique to each owner.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000396

A lock used on the voting system can be evaluated against UL437 door locks and locking cylinders requirements. See *[UL13]* for UL listing for *door locks and locking cylinders* within the standard to review requirements for lockpicking and the attack resistance tests.

The use of a single key used to unlock thousands of precinct-based voting devices makes for a challenging security situation, as copies of this single key design are distributed to a large number of individuals. This creates a situation in which the key can be easily lost or stolen, and subsequently copied. At the same time, this situation does make key management significantly easier for election officials. To alleviate this situation, election officials might want keying schemes that are more or less restrictive in accordance with their election management practices and needs. This system can make use of replicable locks or cylinders, mechanisms which allow for rekeying of locks, or other technologies. The requirement does not mandate a unique key for each piece of voting equipment but requires manufacturers to be able to provide unique keys for the voting equipment if requested by election officials. System owners need to establish procedures for issues such as key reproduction, use, and storage.

12.1-G – Backup power for power-reliant countermeasures

If the voting system uses a powered physical security countermeasure, that physical countermeasure must maintain its state when power is removed and must have a backup power supply. In addition, switching from primary power supply to backup power supply:

1. produces an alert;
2. happens automatically when primary power is unavailable; and
3. generates an event log entry, if possible.

Discussion

This ensures that the countermeasure isn't disabled or intentionally circumvented by a power failure.

Switching to the backup power supply triggers an alarm that alerts an election worker to the issue so that any problem can be further diagnosed and eventually resolved. The alarm can be visible and audible. Once primary power is unavailable, the switch to back up power should be automatic to avoid any gaps in functionality if the switch must be done manually.

If the physical countermeasure leverages the voting system's operating system, it can create an event log entry when it is switched to backup power. The log entry information is security relevant, especially once a security incident has occurred, and would be useful when determining cause. Alternatively, the voting system should log when there is a switch from backup power to the primary power supply.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000397

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

12.2-A – Physical port and access least functionality

The voting system must only expose physical ports and access points that are essential to voting operations, testing, and auditing.

Discussion

Examples of ports are USB and RJ45 physical network interfaces. Examples of access points are doors, and panels, and vents. Voting operations include voting device upgrades and maintenance.

12.2-B – Physical port auto-disable

If a physical connection that supports digital communication between voting system components is broken during an activated or suspended state, the affected voting system port must be automatically disabled.

Discussion

Automatically disabling will require an election worker's attention to re-enable and re-attach any cabling. This remediation is required for continuity and to address any tampering. An added feature could be that the specific election worker performing maintenance is uniquely identified within the logs, but this is not required. This requirement does not include power cabling with a backup power supply or analog accessibility device ports that are used during the activated voting stage.

12.2-C - Physical port restriction

Voting systems must restrict physical access to voting system ports that accommodate removable media, with the exception of ports used to activate a voting session.

Discussion

Physical port access needs to be restricted when not in use. This requirement is not meant to impede the use of accessible technology. This requirement assists in restricting adversaries from adding wireless adapters or other malicious adapters to the voting system.

Although voting systems can have ports dedicated to voting operations outside of election day activities, those ports need not be exposed while balloting is in progress. Removable media (such as Floppy, CD or DVD drives, thumb drives, and memory cards) might be essential to voting operations during pre-voting and post-voting phases of the voting cycle, such as machine upgrade, maintenance, and testing. Therefore, all removable media should be accessible only to authorized personnel. They should not be accessible to voters during activated and suspended phases of the voting cycle. It is

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000398

essential that any removable drives, whether or not they are used by the system, are not accessed without detection.

12.2-D – Disabling ports

Voting systems must allow authorized administrators to logically put physical ports into a disabled state.

Discussion

Logically disabling ports prevents unused ports from being used as a staging point for an attack on the voting system.

12.2-E – Logging enabled and disabled ports

An event log entry that identifies the name of the affected device must be generated when physical ports are enabled or disabled.

Discussion

Whether a port is disabled or not is security relevant, especially once a security incident has occurred, and this information would be useful when determining cause. *12.2-C – Physical port restriction* applies to physical restrictions, whereas *12.2-D – Disabling ports* discusses logical disabling of ports.

Related requirements: 15.1-D – Logging event types

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000399

Principle 13
Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

AMERICAN OVERSIGHT

Principle 13
Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

The requirements for *Principle 13* include ensuring that the voting system prevents unauthorized access to or manipulation of data and records and that the source and integrity of electronic tabulation reports are verifiable. It details cryptographic standards and ensure that the system protects sensitive data that is transmitted over all networks.

The sections in ***Guideline 13.1*** **include**:

1 – Configuration file which deals with the requirement that the system allow only authenticated system administrators to access and modify voting device configuration files. In addition, the election management system (EMS) will uniquely authenticate individuals associated with the role of system administrator before they can access and modify EMS configuration files. Network appliances will uniquely authenticate individuals before allowing them to access and modify configuration files. Configuration files contain important settings, including security settings, and altering them could impact the overall system

2 – Elections records deals with the need for the vote-capture and tabulation system and the EMS to protect the integrity of the cast vote records (CVRs) and ballot images when they are stored in the voting device. These protections should prevent undetectable changes to CVRs and ballot images.

13.2 – Source and integrity of election records covers the requirement that CVRs and ballot images be digitally signed both when stored and before being transmitted. The EMS needs to be able to cryptographically certify all electronic voting records. Digital signatures are a form of integrity protection that can also help trace the source of any updates or alterations to election records.

13.3 – Cryptographic algorithms deals with the requirements that cryptographic functionality be implemented in a cryptographic module validated against *Federal Information Processing Standard (FIPS) 140 [NIST01]*. In addition, cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation. Devices using cryptography need to employ NIST approved algorithms, and the key used with Message Authentication Codes needs to have a specific security strength. Voting system documentation describes how key management is to be performed by election officials.

13.4 – Protecting sensitive data transmission deals with the requirement that data be transmitted by a mutually authenticated connection. Voting systems transmitting data need to

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000401

cryptographically protect the confidentiality and integrity of data sent over a network. A voting system receiving data will adhere to requirements on verifying and logging data received and presenting any verification errors immediately.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000402

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1.1 – Configuration file

13.1.1-A – Authentication to access configuration file

The voting system must allow only authenticated system administrators to access and modify voting device configuration files.

Discussion

Voting system configuration files can include operating system and voting system application configuration files. These files can have a large impact on how the voting system functions and what election logic is being used. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.

Applies to:	Vote-capture and tabulation system
Related requirements:	11.2.1-A – Ensuring authorized access

13.1.1-B – Authentication to access configuration file on EMS

The EMS must uniquely authenticate individuals associated with the role of system administrator before allowing them to access and modify EMS configuration files.

Discussion

EMS configuration files can include operating system and voting system application configuration files. These files can have a large impact on how an EMS tabulates and reports election results. Therefore, accidental or malicious modification can have a large impact on the system and access to these files should be restricted to authorized individuals.

Applies to:	EMS workstation
Related requirements:	11.3.1-C – Multi-factor authentication for administrators 15.1-E – Configuration file access log

13.1.1-C – Authentication to access configuration file for network appliances

Network appliances must uniquely authenticate individuals before allowing them to access and modify configuration files.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000403

Discussion

Network appliances, such as firewalls, routers, switches, and VPN gateways are generally configurable. Individually authenticating users to the device, in lieu of using a shared password, is a standard practice for restricting access to these devices.

Applies to: Network appliance
Related requirements: 11.3.1-A – Access control mechanism application

13.1.2 – Election records

13.1.2-A – Integrity protection for election records

The voting system must integrity prevent modification of CVRs and ballot images when they are stored anywhere within the voting system.

Discussion

Applying access control can help prevent any unauthorized modifications to CVRs and ballot images.

Applying integrity protection ensures that any unauthorized modifications to CVRs and ballot images can be detected.

For example, ballot images can be integrity protected using a private key maintained in a Hardware Security Module and a cryptographic signature of the image.

Related requirements: 13.2-A – Signing stored election records
13.2-B – Verification of election records

AMERICAN OVERSIGHT

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2-A – Signing stored election records

Cast vote records and ballot images must be digitally signed when stored and before being transmitted.

Discussion

Digital signatures address the threat that the records might be tampered with when stored or transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed. Digital signatures also allow verification of the source of any created or modified records. Additional information can be found in *FIPS 186-4 Digital Signature Standard [NIST13c].*

13.2-B – Verification of election records

A voting system must:

1. cryptographically verify the integrity and authenticity of all election data received;
2. immediately log any verification error of received election results;
3. immediately present on-screen any verification errors; and
4. not tabulate or aggregate any data that fails verification.

Discussion

This process of verifying election data and results is a defense in depth measure against accidental errors or a malicious incident regarding modified or false election records. For example, checking the cryptographic integrity of received election results prevents modified election results from being maliciously modified and reported on election night.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000405

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.3-A – Cryptographic module validation

Cryptographic functionality must be implemented in a cryptographic module that meets current FIPS 140 validation, operating in FIPS mode.

This applies to:

1. software cryptographic modules, and
2. hardware cryptographic modules.

Discussion

Use of cryptographic modules validated at level 1 or above ensures that the cryptographic algorithms used are secure and correctly implemented. The current version of *FIPS 140[NIST01, NIST19a]* and information about the *NIST Cryptographic Module Validation Program* are available under *[NIST20e]* in Appendix C: References. Note that a voting device can use more than one cryptographic module, and quite commonly can use a software module for some functions and a hardware module for other functions.

13.3-B – E2E cryptographic voting protocols

Cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation.

Discussion

The cryptographic E2E verifiable voting protocol used by the voting system is subject to the evaluation in requirement *9.1.6-B – Verified Cryptographic Protocol*. Common place cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the *FIPS 140 [NIST01, NIST19a]* validation requirement.

Applies to:	Cryptographic E2E verifiable voting systems
Related requirements:	9.1.6-A – Verified cryptographic protocol

13.3-C – Cryptographic strength

Devices using cryptography must employ NIST approved algorithms with a security strength of at least 112-bits.

Discussion

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000406

At the time of this writing, NIST specifies the security strength of algorithms in SP 800- 57, Part 1 *[NIST20a]*. This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades.

This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.

13.3-D – MAC cryptographic strength

The key used with Message Authentication Codes must also have a security strength of at least 112 bits and use a 96-bit tag length.

Discussion

Message authentication codes of 96-bits are conventional in standardized secure communications protocols, and acceptable to protect voting records and systems.

13.3-E – Cryptographic key management documentation

The voting system documentation must describe how key management is to be performed.

Discussion

This document provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000407

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

13.4-A – Confidentiality and integrity protection of transmitted data

The voting system must:

1. mutually authenticate all network connections;
2. cryptographically protect the confidentiality of all data sent over a network; and
3. cryptographically protect the integrity of all election data sent over the network.

Discussion

Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS. Only wired local area network (LAN) communication, such as ethernet, is possible for *VVSG 2.0* voting systems. This requirement includes network appliances such as switches, firewalls, and routers within its scope.

This does not prevent the use of "double encrypted" connections employing cryptography at multiple layers of the network stack. Data, such as ballot images, must be encrypted before transmission.

Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit can be provided through the use of various protocols, such as IPsec VPNs and SSL/TLS. For more information about TLS implementations, see *NIST SP 800-52 rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations [NIST19b].*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000408

Principle 14
System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.2 - The voting system is designed to limit its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.4 - Voting system software updates are authorized by an administrator prior to installation.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000409

Principle 14
System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

The requirements for *Principle 14* include ensuring that the voting system provides redundancy against security failures, limits its attack surface, maintains and verifies the integrity of all critical components, and authorizes all software updates before they are installed.

14.1 – Documented resiliency against security failures or vulnerabilities covers the requirement that the system's documentation contains a risk assessment which provides technical controls or a notation showing the acceptable risk for each documented threat to system integrity. This document will describe how all controls work together to prevent, mitigate, and respond to attacks on the system. The system will also document necessary processes that must be carried out by election officials or others to ensure the integrity of the system.

14.2 – Designed to limit attack surface requires that the system will prevent extraneous processes and services from being installed or executed and will disable networking and non-essential features. The voting system should not be capable of wireless networking or connecting to external networks. The system will visually show an indicator when networking functionality is enabled and disabled and will follow a secure configuration guide for all underlying operating systems and other voting system components.

The system documentation will include the guidance used to ensure the system is securely configured. The system application will not contain unused or dead code. The system's underlying platform will provide and make use of modern exploit mitigation technologies. The system application will not import entire software libraries where individual functions are more practical. The voting system will have the capability of restricting access to physical ports that are to be used solely by election judges and administrators.

The underlying system platform generally needs to be free of well-known vulnerabilities before certification, unless the certification authority allows it. In that case, a list of these vulnerabilities will be provided to the certification authorities before it is certified.

14.3 – Supply chain covers the requirement that a voting system's documentation contain:

- a supply chain risk management strategy,
- a list of critical components defined by criticality analysis, and
- hardware and software information for the critical components defined in *14.3-B*.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000410

The sections in ***Guideline 14.3*** include:

1 – Boot integrity deals with the requirement that the voting system cryptographically verifies system integrity before the operating system is loaded into memory. If the system fails boot validation, it will not boot, will provide an on-screen alert, and may log this failure along with any information necessary to understand the failure.

2 – Software integrity states that the voting system will only allow digitally signed software and firmware to be installed. The system cryptographically verifies all application running in userspace against an allowlist that identifies all approved and properly installed applications. It will also protect the integrity and authenticity of the allowlist configuration files.

14.4 – Authorized software updates covers the requirement that the voting system authenticates administrators:

- before an operating system update,
- before a software update to the system application and related hardware, and
- before a firmware or driver update.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000411

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.1-A – Risk assessment documentation

The voting system's documentation must contain a risk assessment

Discussion

Risk assessments are a foundation of effective risk management. Additionally, they help to facilitate decision making at the organization, business process, and information system levels. Some decisions may include prioritizing the mitigation or prevention of high risks that are likely to have a high impact an election. Many methods of conducting risk assessments exist, including *NIST SP 800-30-1: Guide for Conducting Risk Assessments [NIST12] or ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management [ISO18d].*

14.1-B – Addressing and accepting risk

The voting system's risk assessment documentation must provide technical controls or a notation showing the acceptance of risk for each documented threat to voting system integrity.

Discussion

Assigning controls or accepting risk is a key part of the risk assessment process. This requirement assists in providing the evidence that a manufacturer has gone through the risk determination process. *NIST SP 800-53* revision 5 *Security and Privacy Controls for Information Systems and Organizations [NIST20h]* can be useful to identify controls that can assist with addressing any identified threats.

14.1-C – System security architecture description

The voting system's risk assessment documentation must describe how physical, technical, and operational controls work together to prevent, mitigate, and respond to attacks on the voting system. This includes the use of:

1. cryptography,
2. malware protection,
3. firewall access control lists, rules, and configurations, and
4. system configurations.

Discussion

Risk assessments can be large, complicated documents. This requirement ensures that a single

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000412

narrative exists to explain to election officials and other system owners how the overall security operates for the voting system.

Related requirements: 3.1.3-C – Physical security

14.1-D – Procedural and operational security

The voting system must document necessary procedural and operational processes that need to occur to ensure integrity of the system.

Discussion

Procedural and operational security processes play a key role in overall system security. If any of these procedures are necessary to ensure system integrity or system security, these practices need to be well documented and explained.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000413

14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2-A – Non-essential networking interfaces

The voting system must disable networking and other features that are non-essential to the function of the voting system by default.

Discussion

When the voting system is booted, networking and other functions are prohibited from running. For instance, networking interfaces such as Wi-Fi and Bluetooth should be disabled.

By disabling features that are non-essential to the voting system, this decreases the attack surface by limiting the functionality and decreasing the entry points that may be accessed by unauthorized users.

14.2-B – Network status indicator

If a voting system has network functionality, the voting system application must visually show an indicator within the management interface when networking functionality is enabled and disabled.

Discussion

This helps to ensure that network functionality is not enabled by accident.

14.2-C – Wireless communication restrictions

Voting systems must not be capable of establishing wireless connections as provided in this section.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, or
- removing wireless hardware within the voting system.

This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used e.g. no wireless drivers present.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000414

This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Related requirements: 8.1-E – Standard audio connectors
15.4-C – Documentation for disabled wireless

14.2-D – Wireless network status indicator

If a voting system has network functionality, the voting system application must visually show an indicator within the management interface to confirm that wireless networking functionality is disabled.

Discussion

Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

14.2-E – External network restrictions

A voting system must not be configured to:

1. establish a connection to an external network, or
2. connect to any device external to the voting system.

Discussion

The basic instructions provided by a vendor should clearly indicate that the intended use and installation of voting systems implements an air gap between the voting system and external networks or external devices. This requirement is intended to limit the voting systems attack surface and disallow connections of the voting system to technologies such as:

- e-pollbooks,
- public switched telephone networks (PSTNs), and
- cellular modems.

In particular, connections to the internet expand the attack surface even further than other wireless technologies because the data traverses over the internet, which reaches all over the world. This type of access allows a malicious actor to attack from various distances, meaning they do not have to be in close proximity of a polling place or near a specific jurisdiction. Exposure to the internet could allow nation-state attackers to gain remote access to the voting system. With remote access an attacker may be able to view all files within a voting system and make modifications to files within the voting system. These files may include election results and ballot records.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000415

This type of exposure could also make voting systems vulnerable to ransomware. Ransomware is a type of malware that could deny access to election data or functionality, usually by encrypting the data with a key known only to the hacker who deployed the malware. Ultimately an attacker could render a voting system non-operational until a ransom is paid.

Related requirements: 15.4-B – Secure configuration documentation

14.2-F – Secure configuration and hardening documentation

The voting system must follow a secure configuration guide for all underlying operating systems and other voting system components, with any deviations from the secure configuration guidance documented and justified.

Discussion

Properly configuring an operating system is a difficult and complex task, with small settings potentially causing a large impact. Industry, NIST, and various agencies within the DoD offer guidance for specific operating systems, as do OS and component manufacturers. Some examples include Security Technical Implementation Guides (STIGs) *[DISA20]* and the Center for Internet Security (CIS) benchmarks.

Documenting deviations ensures that important settings are not overlooked and decisions to deviate are properly considered.

Related requirements: 15.4-B – Secure network configuration documentation

14.2-G – Unused code

The voting system software must not contain unused, or dead code.

Discussion

An attacker may be able to take advantage of the unused code and introduce software bugs/exploits that can be used to make the voting system vulnerable.

Dead code is source code that can never be executed in a running program because the surrounding code makes it impossible for a section of code to ever be executed. See *MITRE CWE-561 [MITRE20]*. Software with dead code is considered poor quality and reduces maintainability.

This requirement does not restrict the use of defensive code, such as exception handling to prevent failures because this code is still traversed to check conditions.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000416

14.2-H – Use of exploit mitigation technologies

The voting system must use exploit mitigation technologies including data execution prevention (DEP) and address space layout randomization (ASLR), or equivalent mitigations.

Discussion

DEP and ASLR are commonplace exploit mitigation technologies that can help prevent a variety of vulnerability types, including memory corruption errors like buffer overflows. If the voting system does not use DEP and ASLR, the equivalent mitigation technologies used must be identified.

Applications need to be written and compiled in such a way as to make use of underlying exploit mitigation technologies.

See the *OWASP Application Security Verification Standard [OWASP19]* for more information about exploit mitigation.

14.2-I – Importing software libraries

The voting system software must import only library components that are necessary.

Discussion

Importing entire software libraries significantly increases the attack surface of the software. Importing only the components of a library, such as modules, functions, or classes needed is a useful attack surface minimization strategy. Following the language's intended import design, such as importing only the specific module needed from a more general "standard" library, will also help with this goal.

This requirement is not intended to encourage developers to avoid the import process by copying code directly to software, which would greatly complicate the update process.

Not all 3rd party libraries are easily modifiable, making this attack surface reduction strategy impractical.

14.2-J – Vulnerability management plan

The voting system documentation must include the plan for how to address vulnerabilities found in the voting system and at minimum include the following:

1. how the voting system design process identifies and addresses well-known vulnerabilities**;**
2. disclosure of all known vulnerabilities within the system,
3. a patch management plan; and
4. the method to receive and send reports of vulnerabilities.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000417

Discussion

This requirement informs how a voting system vendor is able to manage verified vulnerabilities to their voting system.

Certain information can also be included for each vulnerability, such as any severity, impact, or exploitability scores. Tools like the Common Vulnerability Scoring System (CVSS) can be used to communicate the metrics (including the severity) of software vulnerabilities.

For more information about vulnerability and patch management, see *NISTIR 8011 Volume 4, Automation Support for Security Control Assessments: Software Vulnerability Management [NIST20c]* and *NIST SP 800-40, Guide to Enterprise Patch Management Technologies [NIST13b].*

14.2-K – Known vulnerabilities

The underlying voting system platform must be free of well-known vulnerabilities as identified in the vulnerability management plan.

Discussion

Vulnerability scanning tools can be used to identify known vulnerabilities in software and firmware. *The U.S. National Vulnerability Database (NVD)* is one resource that can be useful for identifying known vulnerabilities. Other vulnerability databases also exist and can be leveraged for full vulnerability coverage that might not be identified by automated scanning tools.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000418

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy

The voting system's documentation must contain a supply chain risk management strategy that at minimum includes the following:

1. a reference to the template or standard used, if any, to develop the supply chain risk management strategy;
2. the assurance requirements to mitigate supply chain risks;
3. the contract language that requires suppliers and partners to provide the appropriate information to meet the assurance requirements of the supply chain risk management strategy;
4. the plan for reviewing and auditing suppliers and partners; and
5. the response and recovery plan for a supply chain risk incident.

Discussion

Supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the technology supply chain. These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. These risks can be managed by…

- following *Appendix E* of *NIST SP 800-161 – Supply Chain Risk Management Practices [NIST15b] for Federal Information Systems and Organizations* guidance (Appendix E provides a supply chain management plan(strategy template).
- utilizing the *NIST Cybersecurity Framework Version 1.1 [NIST18c]* by referencing the Supply Chain Risk Management category and subcategory, and
- referencing the relevant security controls for supply chain in *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations [NIST20b].*

Contract language provided must include the products or services acquired from the suppliers/partners and any evidence or artifacts that attest to the required level of assurance.

14.3-B – Criticality analysis

The voting system's documentation must include a list of critical components and suppliers defined by a criticality analysis and supplier impact analysis

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000419

Discussion

Defining the critical components and supplier of the voting system can assist in prioritizing their importance to the voting process and identifying the impact to security, privacy and performance for failure or compromise.

This can be supplemented by following *NISTIR 8179 Criticality Analysis Process Model - Prioritizing Systems and Components [NIST18b]* and *NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks [NIST20d].*

14.3-C – Bill of materials

The voting system's documentation must include the hardware and software information for the critical components defined in the *14.3-B* and at minimum list the following information for each component:

1. component name;
2. manufacturer;
3. model or version; and
4. applicable platform for software (e.g., Windows or Linux).

Discussion

This requirement will use the critical components defined in the critical analysis of *14.3-B – Criticality analysis*. At minimum the bill of materials for critical components are required, but this does not restrict the voting system vendor from listing the bill of materials for other components.

This is a common practice when providing a hardware bill of materials. It is not as common to produce a bill of materials for software and as standards/best practices are developed, they should be considered for inclusion in the software bill of materials.

For more information about the risks of third-party components and developing software bills of materials, see *"Managing Security Risks Inherent in the Use of Third-party Components" [SAFECode19]* and resources from the *National Telecommunications and Information Administration about Software Bills of Materials [NTIA19].*

14.3.1 – Boot integrity

14.3.1-A – Cryptographic boot verification

The voting system must cryptographically verify firmware and software integrity before the operating system is loaded into memory.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000420

Discussion
This requirement does not mandate hardware support for cryptographic verification. This requirement could be met by trusted boot, but other software-based solutions exist. This includes a software bootloader cryptographically verifying the OS prior to execution. Verifying the bootloader itself is excluded from this requirement, but not prohibited.

Applies to: Vote-capture and tabulation device, EMS

14.3.1-B – Preventing of boot on error

If the voting system fails boot validation, the voting system must not boot and provide an onscreen alert.

Discussion
System users need to be notified when the voting system is either corrupted or has been maliciously modified.

Boot validation prevents unauthorized operating systems and software from being installed or run on a system.

Applies to: Vote-capture and tabulation device, EMS

14.3.1-C – Notification of boot validation failure

If the voting system does not pass boot validation, it must present an on-screen alert and provide any other necessary information to understand the failure.

Discussion
Failure of boot validation needs to be provided to users so these errors can be further analyzed when needed. If the voting system is capable of pre-boot logging, failure information could be stored in a log for future analysis.

Applies to: Vote-capture and tabulation device, EMS

14.3.2 – Software integrity

14.3.2-A – Installing software

The voting system must only allow digitally signed software and firmware to be installed.

Discussion
Signed software and firmware ensures that it is not modified before installation, and that it is being distributed by the proper entity.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000421

14.3.2-B – Software verification for installation

The voting system must cryptographically verify the digital signature of software and firmware before it is installed.

Discussion

The security properties of integrity and authenticity are not achieved unless the digital signature for the signed software and firmware is cryptographically verified.

14.3.2-C – Application allowlisting

The voting system must only run applications that have been verified against an allowlist.

Discussion

This requirement helps ensure only authorized applications run on the voting system.

Applies to: Vote-capture device

14.3.2-D – Integrity protection for software allowlists

The voting system must protect the integrity and authenticity of the allowlist configuration files.

Discussion

If the allowlist is improperly modified, the software allowlisting mitigation can be defeated. The most common way of providing allowlist configuration file protection could be a digital signature.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000422

14.4 - Voting system software updates are authorized by an administrator prior to installation.

14.4-A – Authenticated operating system updates

The voting system must authenticate administrators before an operating system update is performed.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless of whether the updated done by a networked method or performed using physical media.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

14.4-B – Authenticated application updates

The voting system must authenticate administrators before a software update to the voting system application and related software.

Discussion
Administrators are required to be authenticated before they can update the voting system, whether the update is applied by a network method or physical media.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

14.4-C – Authenticated firmware updates

The voting system must authenticate administrators before a firmware or driver update.

Discussion
Administrators are required to be authenticated before they can update the voting system, regardless if network enabled update is performed or via physical media.

Related requirements: 11.3.1-B – Multi-factor authentication for critical operations
11.3.1-C – Multi-factor authentication for administrators

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000423

Principle 15
Detection and Monitoring

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.3 - The voting system is designed to protect against malware.

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000424

Principle 15
Detection and Monitoring

The voting system provides mechanisms to detect anomalous or malicious behavior.

The requirements for *Principle 15* include ensuring that voting system equipment records important activities through event logging and generates and reports all error messages as they occur. The system employs mechanisms to protect against malware. Systems with networking capabilities employ defenses against network-based attacks.

15.1 – Event logging covers the requirements that the system be capable of logging events that occur in a voting system and of exporting those logs. The system will not log any information identifying a specific voter or connecting a voter to a specific ballot. At a minimum, the system will log events pertaining to:

- general system functions
- networking
- software, and
- voting functions

In addition, when a system administrator is accessing a configuration file, the system needs to log identifying information about the user accessing that file including the user's, group or role.

15.2 – Error messages occur covers the requirement that systems provide immediate notification to the user when an error occurs as well as logging all errors and creating error reports. The system documentation must include procedures for how election officials should handle errors.

15.3 – Malware protection mechanisms deals with the need for COTS devices that provide EMS functionality to:

- deploy mechanisms to protect against malware,
- promptly notify an election official when malware is detected, and
- provide notification upon the removal or remediation of malware.

The system's malware protection mechanisms need to be updatable and the documentation needs to include the process and procedures for performing the updates. The voting system will log instances when it detects and remediates malware.

15.4 – Defense against network-based attacks deals with the requirement for system documentation to include the network architecture of any internal network used by any portion of the voting system, as well as any documentation needed to explain how wireless capabilities have been disabled within the system. Documentation also lists security relevant configurations and is accompanied by network security best practices, including air-gap procedures to protect sensitive systems from external networks like the internet.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000425

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.1-A – Event logging

The voting system must be capable of logging events that occur in a voting system.

Discussion

The ability to log events within a system allows for continuous monitoring of the voting system. These logs provide a way for administrators to analyze the voting system's activities, diagnose issues, and perform necessary recovery and remediation actions.

15.1-B – Exporting logs

The voting system must be capable of exporting logs.

Discussion

Exporting logs offers the opportunity for external review, clearing storage, and a method to compare with future logs.

15.1-C – Logging voter information

The voting system must not log any information:

1. identifying a specific voter, and
2. connecting a voter to a specific ballot.

Discussion

No voter information is stored anywhere within voting system logs. This would violate voter ballot secrecy because it can link a voter to their ballot selections.

Related requirements: 10.1-A – System use of voter information
11.1-B – Voter information in log files

15.1-D – Logging event types

At minimum, the voting system must log the events included in Table 15-1.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000426

Discussion

Table 15-1 – System events to log provides a list of events that will be included in the voting system event logs. The voting system is not limited to the events in the table.

Logging system events provides insight into general system metrics, errors, and vulnerabilities. Information gathered from logs can be used to improve system performance by preventing future errors/issues or automate issue handling.

Table 15-1 – System events to log

System Event	Description
General system functions	
Device generated error and exception messages	Includes but is not limited to: • The source and disposition of system interrupts resulting in entry into exception handling routines. • Messages generated by exception handlers. • The identification code and number of occurrences for each hardware and software error or failure. • Notification of physical violations of security. • Other exception events such as power failures, failure of critical hardware components, data transmission errors, or other types of operating anomalies. • All faults and the recovery actions taken. Device generated error and exception messages such as ordinary timer system interrupts and normal I/O system interrupts do not need to be logged.
Critical system status messages	Critical system status messages other than information messages displayed by the device during the course of normal operations. Includes but is not limited to: • Diagnostic and status messages upon startup • The “zero totals” check conducted before opening the polling place or counting a precinct centrally • For paper-based systems, the initiation or termination of scanner and communications equipment operation • Printer errors • Detection or remediation of malware or other malicious software • Cryptographic boot validation success/failure

AMERICAN OVERSIGHT

Non-critical status messages	Non-critical status messages that are generated by the device's data quality monitor or by software and hardware condition monitors.
Events that require election official intervention	Events that require election official intervention, so that each election official access can be monitored, and access sequence can be constructed.
Device shutdown and restarts	Both normal and abnormal device shutdowns and restarts.
Changes to system configuration settings	Configuration settings include but are not limited to registry keys, kernel settings, logging settings, and other voting device configuration settings.
Integrity checks for executables, configuration files, data, and logs.	Integrity checks that can indicate possible tampering with files and data.
The addition and deletion of files.	Files that are added or deleted from the voting device.
System readiness results	Includes but is not limited to: • System pass or fail of hardware and software test for system readiness • Identification of the software release, identification of the election to be processed, polling place identification, and the results of the software and hardware diagnostic tests • Pass or fail of ballot style compatibility and integrity test • Pass or fail of system test data removal • Zero totals of data paths and memory locations for vote recording
Removable media events	Removable media that is inserted into or removed from the voting device.
Backup and restore	Successful and failed attempts to perform backups and restores.
Authentication and Access Control	
Authentication related events	Includes but is not limited to: • Login/logoff events (both successful and failed attempts) • Account lockout events • Password changes
Access control related events	Includes but is not limited to: • Use of privileges (such as a user running a process as an administrator)

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000428

	• Attempts to exceed privileges • All access attempts to application and underlying system resources • Changes to the access control configuration of the voting device
User account and role (or groups) management activity	Includes but is not limited to: • Addition and deletion of user accounts and roles • User account and role suspension and reactivation • Changes to account or role security attributes such as password length, access levels, login restrictions, and permissions • Administrator account and role password resets
Networking	
Enabling or disabling networking functionality	Includes but is not limited to: • Wired networking • Wireless networking
Software	
Installing, upgrading, patching, or modifying software or firmware	Logging for installation, upgrading, patching, or modifying software or firmware include logging what was installed, upgraded, or modified as well as a cryptographic hash or other secure identifier of the old and new versions of the data.
Changes to configuration settings	Includes but is not limited to: • Changes to critical function settings. At a minimum, critical function settings include location of election definition file, contents of the election definition file, vote reporting, location of logs, and voting device configuration settings. • Changes to device settings including, but not limited to, enabling and disabling services. • Starting and stopping processes.
Abnormal process exits	All abnormal process exits.
Successful and failed database connection attempts (if a database is used).	All database connection attempts.
Changes to cryptographic keys	At a minimum, critical cryptographic settings include key addition, key removal, and re-keying.
Voting Functions	
Ballot definition and modification	During election definition and ballot preparation, the device can provide logging information for preparing the baseline ballot formats and modifications to them,

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000429

	including a description of the modification and corresponding dates. Includes but is not limited to: • The account name that made the modifications. • A description of what was modified including the file name, location, and the content changed. • The date and time of the modification.
Voting events	Includes: • Opening and closing polls • Casting a vote • Canceling a vote during verification • Success or failure of log and election results exportation • Note: for paper-based devices, these requirements might need to be met procedurally

15.1-E – Configuration file access log

When a system administrator is accessing a configuration file, the voting system must log identifying information of the group or role accessing that file.

Discussion

A record of who modified a configuration file is important for auditing and accountability. The identifying information could include the username or the name of the user for improved traceability.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000430

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.2-A – Presentation of voting application errors

The voting system must provide immediate notification to the user when a voting application error occurs.

Discussion

Voting application errors can disrupt a voter's voting session. Immediate notification of an issue or an error allows for prompt recovery and remediation.

Related requirements: 7.3-A – System-related errors
7.3-K – Warnings, alerts, and instructions

15.2-B – Voting application error handling documentation

The voting system documentation must include procedures for handling voting application errors.

Discussion

Documentation will assist election officials with steps to properly address errors.

Related requirements: 7.3-A – System-related errors
7.3-K – Warnings, alerts, and instructions
15.2-A – Presentation of voting application errors

15.2-C – Logging system errors

The voting system must log system errors.

Discussion

This requirement ensures that any system errors are logged for analysis and remediation. System errors do not include user errors, such as undervotes or overvotes.

Related requirements: 15.1-D – Logging event types

15.2-D – Creating error reports

The voting system must be capable of creating error reports.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000431

Discussion

Error reports allow system administrators to easily analyze the errors that occurred within a system.

15.3 - The voting system is designed to protect against malware.

15.3-A – Malware protection mechanisms

COTS workstations providing EMS functionality must deploy mechanisms to protect against malware.

Discussion

NIST SP 800-83 Revision 1 Guide to Malware Incident Prevention and Handling for Desktops and Laptops [NIST13a] might be useful as supplemental guidance for protecting against malware. Malware protection mechanisms are not required for voter-facing scanners and electronic BMDs. Alternatively, voter-facing scanners and electronic BMDs are required to use protection mechanisms, such as digital signatures and allowlists. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers).

15.3-B – Updatable malware protection mechanisms

The malware protection mechanisms for COTS devices providing EMS functionality must be updatable.

Discussion

Malware protection mechanisms typically use software signatures to identify malware. As new malware signatures are received, the malware protection mechanism needs to be updated with the new signatures to ensure it is identifying all known malware.

Applies to: EMS Workstations, vote-capture and tabulation devices

15.3-C – Documenting malware protection mechanisms

The voting system documentation must include the process and procedures for updating malware protection mechanisms.

Discussion

Providing documentation of the procedures to configure the malware protection mechanisms assists with ensuring the malware protection mechanisms are properly updated to meet *15.3.-B- Updatable malware protection mechanisms.*

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000432

Applies to: EMS Workstations

15.3-D – Notification of malware detection

COTS workstations and servers providing EMS functionality must immediately notify an election official when malware is detected.

Discussion

Malware on an EMS device can disrupt the integrity of the data on the EMS device. Once malware is detected, immediate notification of malware detection allows election officials to promptly take the proper action to avoid data integrity issues. This requirement is focused on EMS COTS workstations and does not include peripheral devices (e.g., printers).

15.3-E – Logging malware detection

The voting system must log instances of detecting malware.

15.3-F – Notification of malware remediation

COTS workstations and servers providing EMS functionality must provide a notification upon the removal or remediation of malware.

Discussion

Once malware it is identified on a device, operations can cease until the malware is remediated. This notification allows administrators and officials to know when it is safe to resume normal operations. This requirement is focused on EMS COTS workstations and does not include peripherals devices (e.g., printers)

15.3-G – Logging malware remediation

The voting system must log malware remediation activities.

Discussion

Remediation that requires the reimaging or reinstallation of the OS, may need to be logged external to the voting system. Prior to reimaging, the malware detection logs could be downloaded and stored on another system to capture the time stamp of the malware event and preserve the malware event log for further analysis.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000433

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practices.

15.4-A – Internal network architecture documentation

The voting system documentation must include the network architecture of any internal network used by any portion of the voting system.

Discussion

Documentation of the internal network architecture can assist with data flow analysis, proper network configuration, and architecture to properly support the voting system.

Applies to: Voting systems with networking capabilities

15.4-B – Secure network configuration documentation

The voting system documentation must list security configurations and be accompanied by network security best practices.

Discussion

This documentation may include how external network services are not included as part of the voting system and are handled through a separate air-gapped process. For example, a sneaker-net process may be used to manually transfer elections results to another system that uses public telecommunications to transmit the unofficial election results to a central count center.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices, these need to be documented and used to the extent practical.

This documentation may also include the use of firewalls and intrusion detection systems (IDS). Firewalls and IDSs are typically used to control and monitor the boundary between a private network and the internet. Although the current requirements do not allow for internet connectivity, firewalls and IDSs may also be used for internal boundaries and monitoring inside a private network. Guidance for Intrusion Detection and prevention systems can be found in *NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems [NIST07].*

Related requirements: 14.2-F – Secure configuration and hardening documentation

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000434

15.4-C – Documentation for disabled wireless

The voting system documentation must include information about how wireless is disabled within the voting system.

Discussion

Documentation for how the voting system is configured to disable wireless networking is important to meet requirement *14.2-D – Wireless network status indicator*, which disallows the use of any wireless connections. Example information for how wireless can be disabled may include the following:

- a system configuration process that disables wireless networking devices,
- disconnecting/unplugging wireless device antennas, and
- removing wireless hardware within the voting system.

A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices exist, these need to be documented and used to the extent practical.

Applies to:	Voting systems with networking capabilities
Related requirements:	14.2-C – Wireless communication restrictions

15.4-D – Rule and policy updates

The voting system must be capable of updating rules and policies for network appliances.

Discussion

Network appliances and the voting system are constantly receiving improvements and information related to current threats. As this information is released, rules and policies might need to be modified to adjust to new capabilities.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000435

Appendix A
Glossary of Terms

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000436

Glossary

A:

absentee ballot

Ballot used for **absentee voting**.
Synonyms: mail ballot, postal ballot

absentee voting

Voting that is typically unsupervised at a location chosen by the **voter** either before or on **election day**.
Synonyms: all-mail voting, mail voting, postal voting, vote-by-mail

access control

The process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities.

accessibility

Measurable characteristics that indicate the degree to which a system is available to, and usable by, individuals with disabilities. The most common disabilities include those associated with vision, hearing, mobility, and cognition.

accreditation

Formal recognition that a laboratory is competent to carry out specific **tests** or calibrations.

activation device

Programmed device that creates credentials necessary to begin a **voting session** using a specific **ballot style**. Examples include **electronic poll books** and card activators that contain credential information necessary to determine the appropriate ballot style for the **voter**.

adjudication

Process of resolving flagged **cast ballots** to reflect **voter intent**. Common reasons for flagging include:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000437

- write-ins,
- **overvotes**,
- marginal **machine-readable mark**,
- having no **contest selections** marked on the entire **ballot**, or
- the ballot being unreadable by a scanner.

administrator

A voting system user with the highest level of access.

Synonyms: admin, highest level of authorized user

air gap

A physical separation between systems that requires data to be moved by some external, manual procedure.

alert time

During a voting session, the amount of time that a **voting device** will wait for detectible **voter** activity after issuing an alert before going into an inactive state requiring **election worker** intervention.

alternative format

The **ballot** or accompanying information is said to be in an alternative format if it is presented in non-standard ballot language and format. Examples include, but are not limited to, languages other than English, Braille, ASCII text, large print, recorded audio.

approval voting

A **vote variation** used for **elections** in which each **voter** may "approve" of (that is, select) any number of **candidates**. Typically, the winner(s) is the most-approved candidate(s).
Synonyms: equal-and-even cumulative voting, proportional voting

assistive technology

A **device** that improves or maintains the capabilities of people with disabilities (such as no vision, low vision, mobility, or cognitive). These devices include headsets, keypads, software, sip-and-puff, and voice synthesizers.

audio format

A **display format** in which information is communicated through sound and speech.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000438

Synonyms: audio ballot

audit

1. Systematic, independent, documented process for obtaining **records**, statements of fact, or other relevant information and assessing them objectively to determine the extent to which specified requirements are fulfilled.
2. Verification of statistical or exact agreement of records from different processes or subsystems of a **voting system**.
3. A review of a system and its controls to determine its operational status and the accuracy of its outputs.

audit trail

Information **recorded** during **election** activities to reconstruct steps followed or to later verify actions taken with respect to the **voting system**. **Audit trails** may include event logs, paper **records**, error messages, and **reports**.

authentication

Verifying the identity of a user, process, or **device**, often as a prerequisite to allowing access to resources in an information system.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000439

B:

ballot

Presentation of the **contest options** for a particular **voter**.

ballot data

A list of **contests** and associated options that may appear on a **ballot** for a particular **election**.

display format

The concrete presentation of the contents of a **ballot** or other information for the voter or election official appropriate to the particular voting technology being used. The contents may be rendered using various methods of presentation (visual or audio), language, or graphics.

ballot image

Archival digital image (e.g. JPEG, PDF, etc.) captured from one or more sides of a paper ballot cast by an individual voter.

ballot instructions

Information provided to the **voter** that describes the procedure for marking the **ballot**. This information may appear directly on the paper or electronic ballot or may be provided separately.

ballot marking device

A **device** that:

- permits **contest options** to be selected and reviewed on an electronic interface,
- produces a human-readable **paper ballot**, and
- does not make any other lasting **record** of the **voter**'s selections.

Synonyms: BMD, EBM, electronic ballot marker

ballot measure

A question that appears on a **ballot** with options, usually in the form of an approval or rejection.
Synonyms: ballot issue, ballot proposition, ballot question, referendum

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000440

ballot measure option

A **contest option** that specifies a response to a **ballot measure**.

ballot rotation

The process of varying the order of listed **candidates** within a **contest**. This allows each candidate to appear first on the list of candidates an approximately equal number of times across different **ballot styles** or **election districts**.

ballot secrecy

A goal of **voting systems** to ensure that no **contest selections** can be associated with a **voter**.

ballot style

Ballot data that has been put into **contest** order for a particular **precinct** or precinct split and considers a particular set of **voter** situations. Voter situations include party affiliation (for **closed primaries**), and age of the voter (in states that permit 17-year-olds to **vote** in **primary elections**), among others.

barcode

An optical, machine-readable representation of data as a sequence of bars or squares or spaces that conform to accepted **standards**. Linear (1d) barcode standards include UPC, EAN and 128. QR is an example of a 2D barcode standard.

batch

A collection of **paper ballots** or ballot images or cast vote records gathered as a group for tabulation or for auditing.

batch-fed scanner

An electronic **voting device** that typically:

- accepts stacks of hand-marked or BMD-produced **paper ballots** and automatically processes them until the stack is empty;
- is usually used at an **election jurisdiction**'s central location;
- is mostly commonly used to process **absentee ballots**;
- usually has input and output hoppers for **ballots**;
- scans a ballot and rejects it if either unreadable or un-processable;
- detects, interprets, and validates **contest selections**;

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000441

- detects and sorts (either digitally or physically) ballots that are unreadable or un-processable, or that contain undeterminable selections, marking exceptions, or write-ins; and
- **tabulates** and **reports** **contest** results as required.

This unit was previously referred to as central count optical scanner or CCOS.
Synonyms: CCOS, central tabulator, central-count optical scanner, high-speed optical scanner

benchmark

Quantitative point of reference to which the measured performance of a system or **device** may be compared.

blank ballot

An issued **ballot** without any selections made.
Synonyms: unmarked ballot

Bluetooth

A wireless protocol that allows two similarly equipped devices to communicate with each other within a short distance, e.g., 30 ft.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000442

C:

callable unit

(Of a software program or logical design) Function, method, operation, subroutine, procedure, or analogous structural unit that appears within a **module**.

candidate

Person contending in a **contest** for **office**. A candidate may be explicitly presented as one of the **contest options** or may be a write-in candidate.

candidate option

A **contest option** that is associated with a **candidate**.

canvass

The process of compiling, reviewing, and validating **election** returns that forms the basis of the official results by a **political subdivision**.

cast

(v) The final action a **voter** takes in selecting **contest options** and irrevocably confirming their intent to **vote** as selected.

cast ballot

Ballot in which the **voter** has taken final action in selecting **contest options** and irrevocably confirmed their intent to **vote** as selected.
Synonyms: voted ballot

cast vote record

Archival tabulatable **record** of a set of **contest selections** produced by a single **voter** as interpreted by the **voting system**.
Synonyms: CVR

central reporting device

Electronic **voting device** that consolidates and **reports** **vote** totals from multiple **precincts** at a central location.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000443

certification testing

Testing of a **voting system** performed by a testing authority (such as the EAC or a state) to ensure that the system meets the requirements defined in the **standards** being tested against in the manner specified in its product documentation.

ciphertext

Data or information in its encrypted form.

closed primary

Partisan primary election in which the **voter** receives a **ballot** containing only those **party-specific contests** pertaining to the **political party** with which the voter is affiliated, along with **non-party-specific contests** presented at the same election. Unaffiliated voters may be permitted to **vote** only on non-party-specific contests.

combined precinct

Two or more **precincts** treated as a single precinct for a specific **election**.
Synonyms: consolidated precinct, super precinct

commercial-off-the-shelf

Hardware or software **components** that are widely available for purchase and can be integrated into special-purpose systems.
Synonyms: COTS

common data format

Standard and practice of creating and storing data in a common, described format that can be read by other systems.
Synonyms: CDF

Common Industry Format

Format used for **usability test** reporting. The format is described in ISO/IEC 25062:2006 "Common Industry Format (CIF) for Usability Test Reports," one of a group of usability **standards**. CIF is the format required for usability test reporting.
Synonyms: CIF

component

Element within a larger **voting system**.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000444

confidentiality

Prevention of unauthorized disclosure of information.

conformance

Fulfilling specified requirements by a product, process, or service.

conformance testing

Process of testing **device** or system of devices against the requirements specified in one or more **standards**. The outcomes of a **conformance test** are generally a pass or fail result, possibly including **reports** of problems encountered during the execution.
Synonyms: conformity assessment

contest

A single decision or set of associated decisions being put before the **voters** (for example, the option of **candidates** to fill a particular public **office** or the approval or disapproval of a constitutional amendment). This term encompasses other terms such as "race," "question," and "issue" that are sometimes used to refer to specific kinds of contests. It does not refer to the legal challenge of an **election** outcome.

contest option

A votable choice that appears under a **contest**.

contest option position

A specified area on a **ballot** where a **voter**'s selection in a particular **contest** can be indicated.
Synonyms: ballot marking target area, ballot selection position, target, target area

contest option vote

Vote that will be **tabulated** for a particular **contest option**.
Synonyms: valid vote

contest selection

A selection made on the **ballot** by a **voter** with respect to a specific single **contest** (for example, a **candidate**, the value "Yes" or "Approve").

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000445

counted ballot

A **read ballot** that has been processed and whose **votes** are included in the vote totals.
Synonyms: tabulated ballot, tallied ballot

cross-party endorsement

Endorsement of a single **candidate** or slate of candidates by more than one **political party**. The candidate or slate appears on the **ballot** representing each endorsing political party.
Synonyms: cross filing

cryptographic end-to-end(E2E) verifiable voting systems

A voting system that uses cryptographic techniques to store an encrypted copy of the voter's ballot selections while maintaining ballot secrecy and allows election outcomes to be independently and universally verified by members of the public. These voting systems provide voters with a special receipt of their cast ballot—one that allows them to verify their vote was included in the outcome but does not reveal to anyone how they voted.
Synonyms: Receipt-based system

cryptographic hash

A cryptographic algorithm that computes a numerical hash value based on a data file or electronic message. It should be infeasible in practice to find two distinct data files or messages that will result in the same numerical hash value. The numerical value can be considered to be a fingerprint of the file or message. Colloquially known as a hash, hash function, or digital fingerprint. Hashes provide integrity protection.

cryptographic key

A numeric value used as input to cryptographic operations, such as **decryption**, **encryption**, signature generation, or verification of a **digital signature**.

cryptography

Discipline that embodies the principles, means, and methods for transforming data to hide their semantic content, prevent their unauthorized use, prevent their undetected modification, or establish their authenticity.

cumulative voting

A **vote variation** used in **multi-seat contests** where a **voter** is permitted to distribute allowed selections to 1 or more **candidates** in whole **vote** increments.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000446

cybersecurity

Measures taken to protect computer systems and data from attack and unauthorized access or use.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000447

D:

decertification

Revocation of national or state certification of a **voting system** or any of its **components**.

decryption

Cryptographic process of transforming encrypted data back into its pre-encryption form.

defense-in-depth

Also called the "Castle" approach. Multiple levels of logical and physical security measures that deny a single point of security **failure** in a system. Examples include the combined use of passwords, **encryption**, lock-and-key access, security seals, and logs.

device

Physical apparatus and any supporting supplies, materials, and logic that together form a functional unit that performs assigned tasks as an integrated whole.

digital certificate

A data set used to identify the holder of the certification and to verify, using a PKI, the authenticity of the certificate. It typically includes the holder's **private key** and is used for cryptographic operations such as digitally signing or encrypting data.

digital signature

A cryptographic operation where a **private key** is used to digitally sign an electronic document and the associated **public key** is used to verify the signature. Digital signatures provide data **authentication** and integrity protection.

direct voter associations

A voter’s personally identifiable information (PII) created or stored by the voting system that can be used to associate a voter with their ballot selections. Examples include first name, last name, address, driver’s license, voter registration number and other PII.
Synonyms: PII

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000448

E:

early voting

Voting that occurs prior to **election day** under the supervision of **election workers**.
Synonyms: in-person absentee voting

elected office

An **office** that is filled primarily or exclusively via **election**.

election

A formal process in which qualified **voters** select **candidates** to fill **seats** in one or more **offices** and/or **vote** on one or more proposed **ballot measures**.

Election Assistance Commission

The Election Assistance Commission, created by the **Help America Vote Act** (HAVA) to assist the states regarding HAVA compliance and to distribute HAVA funds to the states. The EAC is also charged with creating **voting system** guidelines and operating the Federal Government's first voting system certification program. The EAC is also responsible for maintaining the National Voter Registration form, conducting research, and administering a national clearinghouse on **elections** that includes shared practices, information for **voters**, and other resources to improve elections.
Synonyms: EAC

election day

The last day on which **voters** may **cast** a **ballot**. **Absentee ballots** and **early voting** ballots may be cast in advance of election day.

election definition

Data used in defining an **election**, including **election districts**, **contests**, **candidates**, and **ballot style** information.

election definition medium

Programmed memory component containing all applicable **election definition** data required by an election system device.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000449

election district

Administrative area in which **voters** are entitled to **vote** in **contests** that are specific to that area.

election jurisdiction

A geographical area to which an authorized authority has been granted to administer **elections** for political or administrative **offices**. Areas of jurisdiction apply to local, state, and federal levels. States, counties, cities, **towns**, and **townships** are all examples of jurisdictions.

election management system

Set of processing functions and databases within a **voting system** typically used to:

- develop and maintain **election definition** data,
- perform **ballot** layout functions,
- create ballot presentation templates for ballot printers or **devices** used by **voters** for ballot markup,
- **tabulate votes**,
- consolidate and **report** results, and
- maintain **audit trails**.

Synonyms: EMS

election official

Any person who is involved with administering or conducting an **election**, including government personnel and temporary **election workers**. This may include any county clerk and recorder, election judge, member of a **canvassing** board, central election official, **election day** worker, member of a board of county commissioners, member or secretary of a board of directors authorized to conduct public elections, representative of a governing body, or other person engaged in the performance of election duties as required by the election code.

election programming

Process by which **election officials** or their designees use **voting system software** to create the **election definition** and configure all **election definition medium** for use in a specific **election**.

Election Results Reporting System

A system that:

- aggregates and displays **election** results across the **election jurisdiction**,
- can be real-time or near real-time,
- can provide a variety of formats for displaying election results, and

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000450

- may provide direct feeds for the media.

Synonyms: ENR, ERR, election night reporting

election system

1. A technology-based system that is used to collect, process, and store data related to **elections** and election administration. In addition to **voter** registration systems and public election websites, election systems include **voting systems**, **vote** tabulation systems, **electronic poll books**, **election results reporting systems**, and auditing **devices**.
2. Entire array of procedures, people, resources, equipment, and locations associated with conducting elections.

election worker

Any person who interacts with those coming to **vote**. This includes any **poll** worker, **election day** worker, **early voting** worker, or other temporary staff engaged in supporting the voting or vote counting process.
Synonyms: poll worker

electronic ballot interface

Subsystem within a **voting system** which communicates **ballot** information to a **voter** in visual, audio, or other **alternative format** which allows the voter to select **contest options** using vocalization or physical actions.

electronic device

Device that uses electronic or electromechanical **components**.

electronic poll book

Device that partially automates the process of checking in **voters**, assigning them the correct **ballot style**, and marking voters who have been issued a **ballot**. May be used in place of a traditional paper **poll** book. E-poll books can be stand alone at the **precinct** with a separate copy of the registration list or can be networked into a central voter registration system. They can check and update voter **records** in real time.
Synonyms: EPB, e-poll book

eligible voters

The universe of all **voters** who, if they **cast** a **ballot**, would have the legal right to have eligible **contests** on that ballot **tabulated**. This would include those who do not appear in the list of

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000451

eligible voters because they live in a same-day registration or no registration state and did not or could not register ahead of time.

encryption

Cryptographic process of transforming data (called "plaintext") into a form (called "**ciphertext**") that conceals the data's original meaning to prevent it from being known or used. Encryption provides **confidentiality** protection.

endorsement

Approval by a **political party**, for example, as the **candidate** that the party fields in a particular **contest** or as the candidate that should receive straight-party **votes**. In some states, more than one party may endorse a candidate or **contest option**.

enhanced visual format

A **display format** that is an alternative **visual format** supporting personal screen display choices such as text size, color contrast, and preferred language.

extraneous mark

A mark on a **paper ballot** that appears to be unrelated to the act of indicating a **voter**'s selection. Examples include: a mark made unintentionally by a voter that is obviously not related to making a selection; a hesitation mark, a dot within or outside of the **contest option position** made by resting a pen or pencil on the **ballot**; written notes or identifying information not related to indication of the voter's selection; or printing defects.
Synonyms: inadvertent mark, random mark, stray mark

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000452

F:

failure

Looking at **voting system** reliability, a failure is an event that results in:

- loss of one or more functions,
- degradation of performance resulting in a **device** that is unable to perform its intended function,
- automatic reset, restart, or reboot of the **voting device**, operating system or application software, requiring an unanticipated intervention by a person in the role of **election worker** or technician before normal operation can continue, or
- error messages or audit log entries indicating that a failure has occurred.

failure rate

Ratio of the number of **failures** that occur to the volume of data processed.

fault

Flaw in design or implementation that may result in the qualities or behavior of the **voting system** deviating from the qualities or behavior that are anticipated, including those specified in the VVSG or in manufacturer-provided documentation.

Federal Information Processing Standards

Standards for federal computer systems developed by NIST. These **standards** are developed when there are no existing industry standards to address federal requirements for system **interoperability**, portability of data and software, and computer security.
Synonyms: FIPS

finding

(n) Result of a formal evaluation by a **test** lab or accredited expert.
Synonyms: verdict

firewall

A gateway system designed to prevent unauthorized access to a private network or intranet that is connected to the internet. A firewall can be implemented in either **hardware** or software, or a combination of both.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000453

firmware

A specific class of software encoded directly into a **hardware device** that controls its defined functions and provides the low-level control for the device's specific hardware (such as the firmware that initially boots an operating system).

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000454

G:

general election

Election in which all **eligible voters**, regardless of party affiliation, are permitted to select **candidates** to fill public **office** and/or **vote** on **ballot measures**.

graceful recovery

Termination of a process that allows the operating system or parent process to regain normal control. Does not crash the machine or result in a general protection default (GPF) or blue screen. The user is not required to close the application and can continue to use the other functionality.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000455

H:

hardware

The physical, tangible, mechanical, or electromechanical **components** of a system.

Help America Vote Act

Act passed by the U.S. Congress in 2002 to make sweeping reforms to the nation's **voting process**. HAVA addresses improvements to **voting systems** and **voter** access that were identified following the 2000 **election**.
Synonyms: HAVA

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000456

I:

implementation statement

Statement by a **manufacturer** indicating the capabilities, features, and optional functions as well as extensions that have been implemented.
Synonyms: implementation conformance statement

in-person voting

Voting that occurs in an official location under the supervision of **election workers**.

independently

Without assistance from an **election worker** or other person.

indirect voter associations

A unique identifier used to associate a voter with their ballot selections. Indirect associations do not include PII.

information security

Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, **confidentiality**, and availability.
Synonyms: IS

inspection

Examination of a product design, product, process, or installation and determination of its conformity with specific requirements.

interaction mode

Control or navigation option that enables **voters** to operate and interact with the **voting system**, used in conjunction with a display format**.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000457

interoperability

The extent to which systems from different **manufacturers** and **devices** with different system configurations can communicate with each other.

intrusion detection system

A **hardware** or software application that detects and **reports** a suspected security breach, policy violation, or other compromise that may adversely affect the network. Synonyms: IDS

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000458

K:

key management

Activities involving handling of **cryptographic keys** and other related security parameters (such as passwords) during the entire **life cycle** of the keys, including their generation, storage, establishment, entry and output, zeroization, and revocation.

AMERICAN OVERSIGHT

L:

life cycle

Systems engineering concept that identifies the phases that a system passes through, from concept to retirement. There are different concerns and activities associated with each phase of the life cycle.

logic and accuracy testing

Equipment and system readiness **tests** whose purpose is to detect malfunctioning **devices** and improper election-specific setup before the equipment or systems are used in an **election**. **Election officials** conduct L&A tests prior to the start of an election as part of the process of setting up the system and the devices for an election according to jurisdiction practices and conforming to any state laws.
Synonyms: L&A, LAT

limited dexterity mode

An **interaction mode** with **accessibility** features for **voters** with no use of one or both hands or low dexterity. This mode includes the tactile mode and the non-manual mode.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000460

M:

machine-readable mark

Mark in a **contest selection** position of a **paper ballot** that meets requirements for detection by a scanner.

malware

Software or **firmware** intended to perform an unauthorized process that will have adverse impact on the **confidentiality**, integrity, or availability of a system. For example, a virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malware.
Synonyms: malicious code

manually-marked paper ballot

Paper ballot marked by a **voter** using a writing utensil.
Synonyms: MMPB

manufacturer

Entity with ownership and control over a **voting system** submitted for testing.
Synonyms: vendor

marked ballot

Ballot that contains all of the selections made by a **voter**.

message authentication code

A data authenticator generated from the message, usually through cryptographic techniques, that is designed to reveal both accidental errors and intentional modifications of the data. In general, a cryptographic key is also required as an input.
Synonyms: MAC

Misfeed rate

Ratio of the misfeed total to the total **ballot** volume.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000461

module

A structural unit of a software program that serves a specific function for the program or that serves to make the program modular in structure for the purposes of easier understanding and maintenance.

multi-factor authentication

Authentication mechanism requiring two or more of the following:

- something you know (such as a password),
- something you have (such as a **token**),
- something you are (for example, biometric authentication).

multi-seat contest

Contest in which **candidates** are elected to fill a specified number of **seats**.

AMERICAN OVERSIGHT

N:

N-of-M voting

Vote variation in which the **voter** is entitled to allocate a fixed number of **votes** (N) over a list of M **contest options** or **write-in options**, with the constraint that at most 1 vote may be allocated to a given contest option. This usually occurs when multiple **seats** are concurrently being filled in a governing body such as a city council or school board where **candidates** contend for at-large seats. The voter is not obliged to allocate all N votes. 1-of-M is N-of-M voting where N = 1.

National Institute of Standards and Technology

Federal organization tasked with assisting in the development of **voting system standards**. NIST develops and maintains standards for a wide array of technologies. NIST scientists assist the EAC in developing testable standards for voting systems.
Synonyms: NIST

non-manual mode

An interaction mode that use assistive technology, for example, a sip-and-puff switch, to allow voters with no use of their hands to operate the voting system.

non-party-specific contest

Contest where eligibility to **vote** in that contest is independent of **political party** affiliation.

nonvolatile memory

Memory in which information can be stored indefinitely with no external power applied.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000463

O:

office

A position established by law with certain associated rights and duties.

open primary

Partisan primary election in which the **voter** may choose a **political party** at the time of voting and **vote** in **party-specific contests** associated with that party, along with **non-party-specific contests** presented at the same election. Some states require voters to publicly declare their choice of party at the **polling place**, after which the **election worker** provides or activates the appropriate **ballot**. Other states allow the voters to make their choice of party within the privacy of the voting booth.
Synonyms: pick-your-party primary

open source

Computer software with its **source code** (human readable code) made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone and for any purpose. Open source software may:

- be developed in a collaborative public manner;
- be reviewed by multiple professional and amateur programmers;
- require a fee and be licensed like other software; or
- be fully open source or may have only a portion of the software open source.

optical scan

Voting system that **tabulates votes** marked in **contest option positions** or contained with a barcode on the surface of a **paper ballot**.

overseas voter

A U.S. citizen who is living outside of the United States and is eligible to **vote** in their last place of residence in the United States.

overvote

Occurs when the number of selections made by a **voter** in a **contest** is more than the maximum number allowed.
Synonyms: over-vote

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000464

P:

paper ballot

A piece of paper, or multiple sheets of paper, on which all **contest options** of a given **ballot style** are printed.

paper ballot side

The face of a **paper ballot sheet**. A **paper ballot** may have two sides.

paper-based voting system

A voting system that records votes, counts votes, and/or produces a report of the vote count from votes cast on paper cards or sheets

partisan office

Elected office for which **candidates** may appear on the **ballot** with a **political party** designation.

partisan primary

Primary election held to narrow the field of **candidates** in **party-specific contests**.

party-specific contest

Contest where eligibility to **vote** in that contest is restricted based on **political party** affiliation or lack of any affiliation. The affiliation might be the registered affiliation of the **voter** or it might be an affiliation declared at the time of voting.

penetration testing

An evaluation method that enables researchers to search for vulnerabilities in a system. Synonyms: Pen Testing

personal assistive device

Assistive technology belonging to **voters** rather than any supplied with the **voting system**.

personally identifiable information

Any information about an individual including:

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000465

- information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric **records**; and
- any other information that can be linked to an individual, such as medical, educational, financial, and employment information.

Synonyms: PII, voter identifying information, VII

plurality voting

A **vote variation** in which the **candidate** with the most **votes** wins, without necessarily receiving a majority of votes.

political party

An association of individuals under whose name a **candidate** may appear on a **ballot**.

political subdivision

Any unit of government, such as counties, cities, school districts, and water and conservation districts having authority to hold **elections** for public **offices** or on **ballot measures**.

polling place

Location at which **voters** may **cast** in-person **ballots** under the supervision of **election workers** during one or more specific time periods.
Synonyms: poll, polling station

post-election tabulation audit

A post-election **audit** that involves hand-counting a sample of **votes** on paper **records**, then comparing those **counts** to the corresponding vote totals originally **reported**:

- as a check on the accuracy of **election** results, and
- to detect discrepancies using accurate hand counts of the paper records as the **benchmark**.

precinct

Election administration division corresponding to a geographic area that is the basis for determining which **contests** the **voters** legally residing in that area are eligible to **vote** on.
Synonyms: tabulation district, ward

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000466

precinct count

Counting ballots in the same **precinct** in which those **ballots** have been **cast**.

precinct split

A subdivision of a **precinct** which arises when a precinct is split by two or more **election districts** that may require different **ballot styles**.
Synonyms: split, split precinct, sub-precinct

primary election

Election held to determine which **candidates** qualify to appear as **contest options** in subsequent elections.

privacy (for voters)

A property of a **voting system** that is designed and deployed to enable **voters** to obtain a **ballot**, and mark, verify, and **cast** it without revealing their ballot selections or selections of language, display and **interaction modes** to anyone else. This does not preclude the ability of a voter to request assistance under state law.

programmed device

Electronic device that includes software. Most electronic **voting devices** include application logic (software) and are, therefore, programmed devices.

proportional voting

A **vote variation** used in **multi-seat contests** where the **votes** allowed in the **contest** are distributed to the selected **candidates** proportionally depending on the number of selections. This may result in candidates receiving fractional votes.

provisional ballot

A failsafe **ballot** provided to a **voter** whose eligibility for a regular ballot cannot be immediately determined. The ballot may be **counted** or further processed depending on state law.
Synonyms: affidavit ballot

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000467

Q:

quick response code

A 2D, trademarked barcode. An optical, 2-D machine-readable representation of data that conforms to accepted standards.
Synonyms: QR Code

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000468

R:

range voting

A **vote variation** for single-seat **contests**, in which **voters** give each **candidate** a score, the scores are added (or averaged), and the candidate with the highest total is elected.
Synonyms: score voting

ranked choice voting

A **vote variation**:

- which allows each **voter** to rank **contest options** in order of the voter's preference,
- in which **votes** are **counted** in rounds using a series of runoff tabulations to defeat contest options with the fewest votes, and,
- which elects a winner with a majority of final round votes in a single-winner **contest** and provides proportional representation in multi-winner contests.

Synonyms: IRV, RCV, instant run-off voting, ranked order

read ballot

Cast ballot that has been successfully accepted and initially processed, e.g., scanned by an optical scanner.
Synonyms: scanned ballot

recallable ballot

Recorded ballot that can be individually retrieved and included or excluded from further processing.

recertification

Re-examination, and possibly retesting, of a **voting system** that was modified after being previously certified. The object of recertification is to determine if the system as modified still conforms to the requirements.

recorded ballot

A **ballot** for which there is an associated **cast vote record**.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000469

recount

Repeat tabulation of **votes cast** in an **election**, whether manually or electronically, that is used to determine the accuracy of an initial count.

resilience

The ability to recover gracefully from error conditions and unexpected circumstances. For example, manually marked paper preserves evidence of exceptions that can advise both adjudication and audit to achieve better interpretation of original voter intent.

reviewed ballot

Ballot that has been reviewed (either electronically or by the **voter**) before it is **cast**, to determine what **contest selections** it contains.

risk assessment

The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and safeguards that would mitigate this impact.

risk-limiting audit

Post-election tabulation audit procedure for checking a sample of **ballots** (or **voter verifiable records**) that is guaranteed to have a large, pre-specified chance of correcting the **reported** outcome if the reported outcome is wrong (that is, if a full hand count would reveal an outcome different from the reported outcome).
Synonyms: RLA

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000470

S:

seat

An **elected office** position that a single officeholder may occupy for a term of **office**.

security controls

Management, operational, and technical controls (that is, safeguards or countermeasures) prescribed for an information system to protect the **confidentiality**, integrity, and availability of the system and its information.

security strength

A metric associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system.

software independence

Quality of a **voting system** or **voting device** where a previously undetected change or **fault** in software cannot cause an undetectable change or error in **election** outcome. In practice, voting systems are generally viewed as possessing the quality of software independence when they allow for a voter-verifiable paper record of voters' contest selections to be created and compared against vote totals or against an electronic cast vote record used in determining vote totals.
Synonyms: SI

source code

Human readable computer instructions that, when compiled or interpreted, define the functionality of a **programmed device**. Source code can be written by humans or by computers.

standard

A document that provides requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000471

straight-party override

Explicit **voter** selection that overrides or supplements the **vote** selections made by a **straight-party voting** option. Straight-party overrides may be subject to state **election** regulations regarding how they work or whether they are allowed.

straight-party voting

Mechanism that allows **voters** to **cast** a single **vote** to select all **candidates** on the **ballot** from a single **political party**.

support software

Software that aids in developing, maintaining, or using other software, for example, compilers, loaders and other utilities.

switch

An assistive technology primarily used by people with motor impairments to access and control computers and other devices.

secret key cryptography

Encryption system that uses the same key for encryption and **decryption**. This key must be kept secret.

system extent

Administrative unit that is the entire scope within which the **voting system** is used (for example, a county). The system extent corresponds to the top-level reporting context for which the system generates **reports**.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000472

T:

t-coil

Inductive coil used in some hearing aids to allow reception of an audio band magnetic field signal instead of an acoustic signal. The magnetic or inductive mode of reception is commonly used in conjunction with telephones, auditorium loop systems, and other systems that provide the required magnetic field output.

tabulate

Process of totaling **votes**.
Synonyms: count

tabulation report

A **report** containing the counts associated with **ballots** that have been tabulated.

tactile controls

A tactile control is a physical control discernable or perceptible by touch using hands, feet, or other parts of the body. (Does not include touch screens.) Dual switches are a form of tactile controls that can be used by **voters** with minimal use of their hands.

tactile mode

An interaction mode that uses tactile controls to operate the voting system.

tamper-evidence

A feature of a physical or digital artifact that provides evidence of unauthorized modification or access (e.g., tamper-evident seal).

technical data package

Manufacturer documentation relating to the **voting system**, which can include manuals, description of **components**, and details of architectural and engineering design.
Synonyms: TDP

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000473

test

Procedure used to determine one or more characteristics of a given product, process, or service according to a specified procedure for **conformity assessment**. A test may be an operational test or a non-operating test (for example, an **inspection**).

test method

Specified technical procedure for performing a **test**, procedures by which tests are derived, or a combination of these.

Test plan

Document created prior to testing that outlines the scope and nature of testing, items to be **tested**, test approach, resources needed to perform testing, test tasks, risks, and schedule.

third-party logic

Software, **firmware**, or hardwired logic that is neither application logic nor **COTS**. This includes, for example, general-purpose software developed by a third party that is either customized (for example, ported to a new platform, as is Windows Embedded Compact), not widely used, or source-code generated by a COTS package.

token

Something a user possesses and controls, typically a key or password, that is used to authenticate an identity.
Synonyms: authentication token, cryptographic token

touch mode

Interaction mode that uses a touch screen to operate the voting system.

touch screen voting machine

A **vote-capture device** that utilizes a computer screen to display the **ballot** and allows the **voter** to indicate their selections by touching designated locations on the screen.

town

An urban area that has a name, defined boundaries, and local government, and that is generally larger than a village and smaller than a city. Term used in New England, New York, and Wisconsin to refer to the equivalent of the civil township in these states.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000474

township

A widely used unit of local government in the United States, subordinate to a county, with some form of local government for which it generally conducts **elections**.
Synonyms: civil township

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000475

U:

undervote

Occurs when the number of **voter** selections in a **contest** is less than the maximum number allowed for that contest or when no selection is made. The number of undervotes is equal to the number of **votes** lost, for example, if no selection is made in a vote for two contest the number of votes lost is two.
Synonyms: under-vote

Uniformed and Overseas Citizens Absentee Voting Act

Act of Congress in 1986 requiring that the states and territories allow certain groups of citizens to register and **vote** absentee in **elections** for Federal **offices**.
Synonyms: UOCAVA

UOCAVA voter

An overseas voter or an active-duty member of the U.S. military, either within or outside the United States, including any accompanying spouse and family members who are eligible to **vote** in their last place of residence in the United States. The **Uniformed and Overseas Citizens Absentee Voting Act** is commonly referred to as UOCAVA.

usability

Effectiveness, efficiency, and satisfaction with which a specified set of users can achieve a specified set of tasks in a particular environment. Usability in the context of **voting** refers to **voters** being able to **cast valid votes** as they intended quickly, without errors, and with confidence that their **contest selections** were **recorded** correctly. It also refers to the usability of the setup and operation of voting equipment in the **polling place**.

usability testing

Testing that encompasses a range of methods that examine how users in the target audience actually interact with a system, in contrast to analytic techniques such as usability inspection**.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000476

V:

validation

Process of evaluating a system or **component** during or at the end of the development process to determine whether it satisfies specified requirements.

visual format

A **display format** in which information is displayed on screen or paper for perception using sight.

vote

Indication of support for a particular **contest option**.

vote center

A physical location where **voters** from multiple **precincts** may **cast** their **ballots**.

vote variation

Voting style or feature, including but not limited to the following**:** approval voting**,** Borda count, cumulative voting, N**-**of-M voting**,** plurality voting**,** proportional voting**,** range voting, and ranked choice voting.

vote-by-mail

Method of voting by which **eligible voters** are **mailed ballots** and information packets by the local **election jurisdiction**. **Voters** may be able to return their **marked ballots** by mail, bring them to an election office, or drop them off in secure drop boxes.
Synonyms: VBM, all-mail voting, mail voting, postal voting

vote-capture device

Component of a voting system that captures and/or counts voter selections from paper or electronic ballots. Vote-capture devices may or may not be directly voter-facing; voter-facing vote-capture devices include ballot marking devices and voter-facing scanners, while non-voter facing vote-capture devices include batch-fed scanners.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000477

voter

Person permitted to **cast** a **ballot**.

voter intent

A cognitive construct, formed by the **voter**, that they attempt to express through actions taken to mark, verify, and **cast** the issued **ballot**.

voter verifiable

A **voting system** feature that provides the **voter** an opportunity to verify that their **contest selections** are being **recorded** correctly before the **ballot** is **cast**.

voter verified paper record

A paper document that the **voter** can review before officially **casting** their **ballot**.
Synonyms: VVPR

voter-facing scanner

An electronic **voting device** that:

- accepts hand-marked or BMD-produced **paper ballots** one sheet at a time;
- is usually used for **in-person voting**;
- permits **election workers** to open and close the **polls**;
- scans a **ballot** and rejects it if either unreadable or un-processable;
- detects, interprets and validates **contest selections**;
- notifies the **voter** of voting exceptions (such as **undervotes** or **overvotes**) or unreadable marks;
- stores accepted ballots in a secure container;
- sorts or otherwise marks ballots or **ballot images** that need subsequent human review; and
- **tabulates** and **reports** **contest** results after polls are closed.

This unit was previously referred to as **precinct count** optical scanner or PCOS.
Synonyms: PCOS, precinct-count optical scanner

voting device

Device that is part of the **voting system**.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000478

voting process

Entire array of procedures, people, resources, equipment, and locations associated with conducting **elections**.

voting session

A collection of activities including **ballot** issuance, **voter** interaction with the **vote-capture device**, voting, verification, and casting.

voting station

The location within a **polling place** where **voters** may **record** their **votes**. A voting station includes the area, location, booth, or enclosure where voting takes place.

voting system

Equipment (including hardware, firmware, and software), materials, and documentation used to enact the following functions of an election:

1. define elections and ballot styles,
2. configure voting equipment,
3. identify and validate voting equipment configurations,
4. perform logic and accuracy tests,
5. activate ballots for voters,
6. record votes cast by voters,
7. count votes,
8. label ballots needing special treatment,
9. generate reports,
10. export election data including election results,
11. archive election data, and
12. produce records in support of audits.

voting system software

The executable code and associated configuration files needed for the proper operation of the **voting system**.

voting system test lab

Privately owned testing laboratories that **test voting systems** (and other **election systems**) for **conformance** to the Voluntary Voting System Guidelines (VVSG) or to other requirements, including individual state requirements. VSTLs are periodically reviewed for conformance to

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000479

National Voluntary Laboratory Accreditation Program (NVLAP) administered by the National Institute for Standards and Technology (NIST).
Synonyms: VSTL

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000480

W:

write-in option

A type of **contest option** that allows a **voter** to specify a **candidate**, usually not already listed as a contest option. Depending on **election jurisdiction** rules, in some cases only previously approved names will be considered as valid write-in **contest selections**.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000481

Appendix B
Requirements Listing

Requirements Listing

The VVSG 2.0 - Principles and Guidelines

Principle 1: High Quality Design
Principle 2: High Quality Implementation
Principle 3: Transparent
Principle 4: Interoperable
Principle 5: Equivalent and Consistent Voter Access
Principle 6: Voter Privacy
Principle 7: Marked, Verified, and Cast as Intended
Principle 8: Robust, Safe, Usable, and Accessible
Principle 9: Auditable
Principle 10: Ballot Secrecy
Principle 11: Access Control
Principle 12: Physical Security
Principle 13: Data Protection
Principle 14: System Integrity
Principle 15: Detection and Monitoring

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000482

Principle 1: High Quality Design

The voting system is designed to accurately, completely, and robustly carry out election processes.

1.1 – The voting system is designed using commonly-accepted election process specifications.

1.1.1 – Election definition
1.1.1-A – Election definition
1.1.1-B – Serve multiple or split precincts and election districts
1.1.1-C – Multiple identifiers
1.1.1-D – Definition of parties and contests
1.1.1-E – Voting variations
1.1.1-F – Confirm recording of election definition
1.1.1-G – Election definition distribution
1.1.1-H – Jurisdiction-dependent content
1.1.1-I – Include contests
1.1.1-J – Exclude contests
1.1.1-K – Primary elections, associate contests with parties
1.1.1-L – Ballot rotation, Election definition
1.1.1-M – Ballot configuration in combined or split precincts
1.1.1-N – Ballot style identification

1.1.2 – Pre-election testing
1.1.2-A – Built-in self-test and diagnostics
1.1.2-B – Installation of software and ballot styles
1.1.2-C – Use of test ballots
1.1.2-D – Testing all ballot positions
1.1.2-E – Testing cast vote record creation
1.1.2-F – Testing codes and image creation
1.1.2-G – Testing equipment calibration
1.1.2-H – No side-effects from pre-election testing
1.1.2-I – Equipment status and readiness reports
1.1.2-J – Ballot style readiness reports
1.1.2-K – Precinct-based voting devices readiness reports
1.1.2-L – All vote-capture devices readiness reports

1.1.3 – Opening the polls
1.1.3-A – Opening the polls
1.1.3-B – Non-zero totals

1.1.4 - Casting
1.1.4-A – Voting and casting the ballot
1.1.4-B – Control ballot configuration
1.1.4-C – Precinct splits, Casting
1.1.4-D – Ballot rotation, Casting
1.1.4-E – Partisan closed primary ballot
1.1.4-F – Partisan open primary ballot
1.1.4-G – Indicate party affiliations and endorsements
1.1.4-H – Write-in contest options
1.1.4-I – Write-in reconciliation
1.1.4-J – N-of-M contest, Casting
1.1.4-K – Straight-party voting, Casting
1.1.4-L – Cumulative voting contest, Casting
1.1.4-M – Ranked choice voting contest, Casting
1.1.4-N – Party preference contest
1.1.4-O – Top-2 primary contest (blanket primary contest)
1.1.4-P – Presidential delegate contest, Casting
1.1.4-Q – Proportional voting contest (equal-and-even cumulative voting contest), Casting
1.1.4-R – Group voting contest, Casting
1.1.4-S – Top-2 IRV contest (supplementary or contingent vote contest)

1.1.5 – Recording voter choices
1.1.5-A – Casting and recording
1.1.5-B – Ballot orientation
1.1.5-C – Record contest selection information
1.1.5-D – Record write-in information
1.1.5-E – Record election and contest information
1.1.5-F – Record ballot selection override information
1.1.5-G – Record audit information
1.1.5-H – Store and link corresponding image

1.1.6 – Ballot handling for vote-capture devices
1.1.6-A – Detect and prevent ballot style mismatches
1.1.6-B – Detect and reject ballots that are oriented incorrectly
1.1.6-C – Ballot separation when batch feeding
1.1.6-D – Overvotes, undervotes, blank ballots
1.1.6-E – Write-ins, Ballot handling for vote-capture devices
1.1.6-F – Ability to clear mis-fed ballots
1.1.6-G – Scan to manufacturer specifications
1.1.6-H – Accurately detect imperfect marks
1.1.6-I – Ignore extraneous marks inside voting targets
1.1.6-J – Marginal marks, without bias
1.1.6-K – Repeatability

1.1.7 – Exiting or suspending voting
1.1.7-A – Exiting or suspending election mode
1.1.7-B – No voting when voting is stopped
1.1.7-C – Voting stop integrity check
1.1.7-D – Report on voting stop process
1.1.7-E – Prevent re-entering election mode

1.1.8 – Tabulation
1.1.8-A – Tabulation
1.1.8-B – Partisan primary elections
1.1.8-B.1 – Tabulation of a closed primary ballot
1.1.8-B.2 – Tabulation of an open primary ballot
1.1.8-B.3 – Open primary ballot with party preference contest
1.1.8-C – Write-ins, Tabulation
1.1.8-D – Ballot rotation, Tabulation
1.1.8-E – Straight-party voting, Tabulation
1.1.8-F – Cross-party endorsement with straight-party voting
1.1.8-G – Precinct splits, Tabulation

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000483

1.1.8-H – N-of-M contest, Tabulation
1.1.8-I – Cumulative voting contest, Tabulation
1.1.8-J – Ranked choice voting contest, Tabulation
1.1.8-K – Group voting contest, Tabulation
1.1.8-L – Presidential delegate contest, Tabulation
1.1.8-M – Recall contest pair
1.1.8-N – Proportional voting contest (equal-and-even cumulative voting contest), Tabulation
1.1.9 – Reporting results
1.1.9-A – Post-election reports
1.1.9-B – Report categories of cast ballots
1.1.9-C – Report categories of votes
1.1.9-D – Reporting combined or split precincts
1.1.9-E – Report counted ballots by contest
1.1.9-F – Report votes for each contest option
1.1.9-G – Report overvotes for each contest
1.1.9-H – Report undervotes for each contest
1.1.9-I – Ranked choice voting, report results
1.1.9-J – Precinct reporting devices, reporting device consolidation
1.1.9-K – Precinct reporting devices, no tallies before polls close
1.1.9-L – Report read ballots by party
1.1.9-M – Reports are time stamped

1.2 – The voting system is designed to function correctly under real-world operating conditions.

1.2 – Assessment of accuracy
1.2-A – Assessment of accuracy
1.2-B – Reliably detectable marks
1.2-C – Minimum ballot positions
1.2-D – Handle maximum volume
1.2-E – Respond gracefully to stress of system limits
1.2-F – No single point of failure
1.2-G – Misfeed rate benchmark
1.2-H – Protect against failure of input and storage devices
1.2-I – FCC Part 15 Class A and B conformance
1.2-J – Power supply from energy service provider
1.2-K – Power port connection to the facility power supply
1.2-L – Leakage from grounding port

1.3 – Voting system design supports evaluation methods enabling testers to clearly distinguish systems that correctly implement specified properties from those that do not.

1.3-A – Reporting of manufacturer-performed tests
1.3-B – Coverage of manufacturer-performed tests

Principle 2: High Quality Implementation

The voting system is implemented using high quality best practices.

2.1 - The voting system and its software are implemented using trustworthy materials and best practices in software development.

2.1 – Software quality
2.1-A – Acceptable programming languages
2.1-B – COTS language extensions are acceptable
2.1-C – Acceptable coding conventions
2.1-D – Records last at least 22 months
2.1.1 – Workmanship
2.1.1-A – General build quality
2.1.1-B – Durability estimation
2.1.1-C – Durability of paper
2.1.1-D – Ensure compatibility of specified paper and ink
2.1.2 – Maintainability
2.1.2-A – Electronic device maintainability
2.1.2-B – System maintainability
2.1.2-C – Nameplate and labels

2.2 – The voting system is implemented using best practice user-centered design methods that consider a wide range of representative voters, including those with and without disabilities, and election workers.

2.2 – Design and implementation process
2.2-A – User-centered design process

AMERICAN OVERSIGHT

2.3 - Voting system logic is clear, meaningful, and well-structured.

2.3 – Voting system logic
2.3-A – Block-structured exception handling
2.3-B – Legacy library units
2.3-C – Separation of code and data
2.3-D – Hard-coded passwords and keys

2.3.1 – Software flow
2.3.1-A – Unstructured control flow
2.3.1-B – Goto
2.3.1-C – Intentional exceptions
2.3.1-D – Unstructured exception handling

2.4 - Voting system structure is modular, scalable, and robust.

2.4 – Modularity
2.4-A – Modularity
2.4-B – Module testability
2.4-C – Module size and identification
2.4-D – Large data structures in separate files

2.5 - The voting system supports system processes and data with integrity.

2.5 – System processes and data
2.5-A – Self-modifying code
2.5-B – Unsafe concurrency

2.5.1 – Code integrity
2.5.1-A – COTS compilers
2.5.1-B – Interpreted code, specific COTS interpreter
2.5.1-C – Prevent tampering with code
2.5.1-D – Prevent tampering with data

2.5.2 – Input/output errors
2.5.2-A - Input validation and error defense

2.5.3 – Output protection
2.5.3-A – Escaping and encoding output
2.5.3-B – Sanitize output
2.5.3-C – Stored injection

2.5.4 – Error handling
2.5.4-A – Mandatory internal error checking
2.5.4-B – Array overflows
2.5.4-C – Buffer overflows
2.5.4-D – CPU traps
2.5.4-E – Garbage input parameters
2.5.4-F – Numeric overflows
2.5.4-G – Uncontrolled format strings
2.5.4-H – Recommended internal error checking
2.5.4-I – Pointers
2.5.4-J – Memory mismanagement
2.5.4-K – Nullify freed pointers
2.5.4-L – React to errors detected
2.5.4-M – Election integrity monitoring
2.5.4-N – SQL injection
2.5.4-O – Parameterized queries

2.6 - The voting system handles errors robustly and gracefully recovers from failure.

2.6 – Graceful recovery
2.6-A – Surviving device failure
2.6-B – No compromising voting or audit data
2.6-C – Coherent checkpoints

2.7 - The voting system performs reliably in anticipated physical environments.

2.7 – Physical environments
2.7-A – Assessment of reliability
2.7-B – Continuous operation – typical environmental conditions
2.7-C – Continuous operation – varied environmental conditions
2.7-D – Ability to support maintenance and repair physical environment conditions – non-operating
2.7-E – Ability to support transport and storage physical environment conditions – non-operating
2.7-F – Ability to support storage temperatures in physical environment – non-operating
2.7-G – Electrical disturbances
2.7-H – Power outages, sags, and swells
2.7-I – Withstand conducted electrical disturbances
2.7-J – Emissions from other connected equipment
2.7-K – Electrostatic discharge immunity

AMERICAN OVERSIGHT

Principle 3: Transparent

The voting system and voting processes are designed to provide transparency.

3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.1.1 – System overview documentation
3.1.1-A – System overview documentation
3.1.1-B – System overview, functional diagram
3.1.1-C – System description
3.1.1-D – Identify software and firmware by origin
3.1.1-E – Traceability of procured software

3.1.2 – System performance documentation
3.1.2-A – System performance documentation
3.1.2-B – Maximum tabulation rate
3.1.2-C – Reliably detectable marks
3.1.2-D – Processing capabilities

3.1.3 – System security documentation
3.1.3-A – System security documentation
3.1.3-B – Access control implementation
3.1.3-C – Physical security
3.1.3-D – Audit procedures

3.1.4 – Software installation documentation
3.1.4-A – Software installation documentation
3.1.4-B – Software information
3.1.4-C – Software location information
3.1.4-D – Election specific software identification
3.1.4-E – Installation software and hardware
3.1.4-F – Software installation procedures
3.1.4-G – Baseline image creation
3.1.4-H – Programmed device configuration replication
3.1.4-I – Software installation record creation
3.1.4-J – Procurement of voting system software
3.1.4-K – Open market procurement of COTS software
3.1.4-L – Erasable storage media preparation
3.1.4-M – Trusted storage media

3.1.5 – System operations documentation
3.1.5-A – System operations documentation
3.1.5-B – Support training
3.1.5-C – Functions and modes
3.1.5-D – Roles
3.1.5-E – Conditional actions
3.1.5-F – References
3.1.5-G – Operational environment
3.1.5-H – Readiness testing
3.1.5-I – Features
3.1.5-J – Support
3.1.5-K – Transportation and storage

3.1.6 – System maintenance documentation
3.1.6-A – System maintenance documentation
3.1.6-B – General contents
3.1.6-C – Maintenance viewpoint
3.1.6-D – Equipment overview details
3.1.6-E – Maintenance procedures
3.1.6-F – Preventive maintenance procedures
3.1.6-G – Troubleshooting procedure details
3.1.6-H – Special equipment
3.1.6-I – Parts and materials
3.1.6-J – Approved parts list
3.1.6-K – Marking devices
3.1.6-L – Approved manufacturers
3.1.6-M – Ballot stock specification
3.1.6-N – Ballot stock specification criteria
3.1.6-O – Printer paper specification
3.1.6-P – System maintenance, maintenance environment
3.1.6-Q – System maintenance, maintenance support and spares

3.1.7 – Training documentation
3.1.7-A – Training documentation
3.1.7-B – Personnel
3.1.7-C – User functions versus manufacturer functions
3.1.7-D – Training requirements

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000486

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.2 – Setup inspection documentation

3.2-A – Setup inspection process
3.2-B – Minimum properties included in the setup inspection process
3.2-C – Setup inspection record generation
3.2-D – Installed software identification procedure
3.2-E – Software integrity verification procedure
3.2-F – Election information value
3.2-G – Maximum and minimum values of election information storage locations
3.2-H – Variable value inspection procedure
3.2-I – Backup power operational range
3.2-J – Backup power inspection procedure
3.2-K – Cabling connectivity inspection procedure
3.2-L – Communications operational status inspection procedure
3.2-M – Communications on/off status inspection procedure
3.2-N – Quantity of voting equipment
3.2-O – Consumable inspection procedure
3.2-P – Calibration of voting device components
3.2-Q – Checklist of properties to be inspected

3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.

3.3 – Public documentation

3.3-A – System security, system event logging
3.3-B – Specification of common data format usage
3.3-C – Bar and other codes
3.3-D – Ballot selection codes

Principle 4: Interoperable

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals.

4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.1 – Interoperable formats

4.1-A – Election programming data input and output
4.1-B – Tabulator report data
4.1-C – Exchange of cast vote records (CVRs)
4.1-D – Exchange of voting device election event logs
4.1-E – Voting device event code documentation
4.1-F – Specification of common format usage

4.2 - Standard, publicly available formats for other types of data not addressed by CDF specifications are used.

4.2 – Standard formats

4.2-A – Standard formats
4.2-B – Public documented manufacturer formats

4.3 - Widely-used hardware interfaces and communications protocols are used.

4.3 – Interfaces and communication protocols

4.3-A – Standard device interfaces

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000487

4.4 - Commercial-off-the-shelf (COTS) devices can be used if they meet all applicable VVSG requirements.

4.4 – COTS

4.4-A – COTS devices meet applicable requirements

Principle 5: Equivalent and Consistent

All voters can access and use the voting system regardless of their abilities.

5.1 – Voters have a consistent experience throughout the voting process within any method of voting.

5.1 – Consistent experience

5.1-A – Voting methods and interaction modes

5.1-B – Languages

5.1-C – Vote records

5.1-D – Accessibility features

5.1-E – Reading paper ballots

5.1-F – Accessibility documentation

5.2 – Voters receive equivalent information and options in all modes of voting.

5.2 – Equivalent information

5.2-A – No bias

5.2-B – Presenting content in all languages

5.2-C – Information in all modes

5.2-D – Audio synchronized

5.2-E – Sound cues

5.2-F – Preserving votes

Principle 6: Voter Privacy

Voters can mark, verify, and cast their ballot privately and independently.

6.1 - The voting process preserves the privacy of the voter's interaction with the ballot, modes of voting, and vote selections.

6.1 – Privacy of interaction

6.1-A – Preserving privacy for voters

6.1-B – Warnings

6.1-C – Enabling or disabling output

6.1.D – Audio privacy

6.2 - Voters can mark, verify, and cast their ballot or other associated cast vote record without assistance from others.

6.2-A - Voter independence

Principle 7: Marked, Verified, and Cast as Intended

Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.

7.1 – The default voting system settings present a ballot usable for the widest range of voters, and voters can adjust settings and preferences to meet their needs.

7.1 – Default settings

7.1-A – Reset to default settings

7.1-B – Reset by voter

7.1-C – Default contrast

7.1-D – Contrast options

7.1-E – Color conventions

7.1-F – Using color

7.1-G – Text size (electronic display)

7.1-H – Scaling and zooming (electronic display)

7.1-I – Text size (paper)

7.1-J – Sans-serif font

7.1-K – Audio settings

7.1-L – Speech frequencies

7.1-M – Audio comprehension

7.1-N – Tactile keys

7.1-O – Toggle keys

7.1-P – Identifying controls

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000488

7.2 – Voters and election workers can use all controls accurately, and voters have direct control of all ballot changes.

7.2 – Controls
7.2-A – Display and interaction options
7.2-B – Navigation between contests
7.2-C – Voter control
7.2-D – Scrolling
7.2-E – Touch screen gestures
7.2-F – Voter speech
7.2.G – Voter control of audio
7.2-H – Accidental activation
7.2.-I – Touch area size
7.2-J – Paper ballot target areas
7.2-K – Key operability
7.2-L – Bodily contact
7.2-M – No repetitive activation
7.2-N – System response time
7.2-O – Inactivity alerts
7.2-P – Floor space
7.2-Q – Physical dimensions
7.2-R – Control labels visible

7.3 – Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

7.3 – Understandable information
7.3-A – System-related errors
7.3-B – No split contests
7.3-C – Contest information
7.3-D – Consistent relationship
7.3-E – Feedback
7.3-F – Correcting the ballot
7.3-G – Full ballot selections review
7.3-H – Overvotes
7.3-I – Undervotes
7.3-J – Notification of casting
7.3-K – Warnings, alerts, and instructions
7.3-L – Icon labels
7.3-M – Identifying languages
7.3-N – Instructions for voters
7.3-O – Instructions for election workers
7.3-P – Plain language

Principle 8: Robust, Safe, Usable, and Accessible

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 – The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.1 – Protect from harmful conditions
8.1-A – Electronic display screens
8.1-B – Flashing
8.1-C – Personal Assistive Technology (PAT)
8.1-D – Secondary ID and biometrics
8.1-E – Standard audio connectors
8.1-F – Discernable audio jacks
8.1-G – Telephone style handset
8.1-H – Sanitized headphones
8.1-I – Standard PAT jacks
8.1-J – Hearing aids
8.1-K – Eliminating hazards

8.2 – The voting system meets currently accepted federal standards for accessibility.

8.2-A – Federal standards for accessibility

8.3 – The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities.

8.3-A – Usability tests with voters

8.4 – The voting system is evaluated for usability with election workers.

8.4-A – Usability tests with election workers

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000489

Principle 9: Auditable

The voting system is auditable and enables evidence-based elections.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.1 – Software independence
9.1.1-A – Software independent
9.1.2 – Tamper-evidence
9.1.2-A – Tamper-evident records
9.1.2-B – Tamper-evident record creation
9.1.3 – Voter verification
9.1.3-A – Records for voter verification
9.1.3-B – Ballot error correction
9.1.3-C – Voter reported errors
9.1.4 – Auditable
9.1.4-A – Auditor verification
9.1.4-B – Documented procedure
9.1.5 – Paper records
9.1.5-A – Paper record production
9.1.5-B – Paper record retention
9.1.5-C – Paper record intelligibility
9.1.5-D – Matching selections
9.1.5-E – Paper record transparency and interoperability
9.1.5-F – Unique identifier
9.1.5-G –Preserving software independence
9.1.6 – Cryptographic E2E verifiable
9.1.6-A– Verified cryptographic protocol
9.1.6-B – Independent evaluation of E2E cryptographic protocol implementation
9.1.6-C – Cryptographic ballot selection verification by voter
9.1.6-D – Methods for cryptographic ballot selection verification
9.1.6-E – Ballot receipt
9.1.6-F – Disputes involving ballot receipts
9.1.6-G – Evidence export
9.1.6-H– Mandatory ballot availability
9.1.6-I – Verification of encoded votes documentation
9.1.6-J – Verifier reference implementation
9.1.6-K – Privacy preserving, universally verifiable ballot tabulation

9.2 - The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities.

9.2-A – Audit support documentation

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-A – Data protection requirements for audit records

9.4 - The voting system supports efficient audits.

9.4 – Efficient audits
9.4-A – Risk-limiting audit
9.4-B – Random numbers supporting audit processes
9.4-C – Unique ballot identifiers
9.4-D – Multipage ballots

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000490

Principle 10: Ballot Secrecy

The voting system protects the secrecy of voters' ballot selections.

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System use of voter information

10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

10.2.1 – Voter associations
10.2.1-A – Direct voter associations
10.2.1-B – Indirect voter associations
10.2.1-C – Use of indirect voter associations
10.2.1-D – Isolated storage location
10.2.1-E – Removal of indirect voter associations
10.2.1-F – Confidentiality for ballots with indirect voter associations
10.2.2 – Identification in vote records
10.2.2-A – Identifiers used for audits
10.2.2-B – No voter record order information
10.2.2-C – Identifying information in voter record file names
10.2.2-D – Aggregating and ordering
10.2.2-E – Randomly generated identifiers
10.2.3 – Access to cast vote records (CVR)
10.2.3-A – Restrict access to records of voter intent
10.2.3-B – Digital voter record access log
10.2.4 – Voter information in other devices and artifacts
10.2.4-A – Voting information in receipts
10.2.4-B – Logging of ballot selections
10.2.4-C – Activation device records

Principle 11: Access Control

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

11.1 - The voting system enables logging, monitoring, reviewing, and modifying of access privileges, accounts, activities, and authorizations.

11.1 – Access privileges
11.1-A – Logging activities and resource access
11.1-B – Voter information in log files
11.1-C – Preserving log integrity
11.1-D – On-demand access to logs

11.2 - The voting system limits the access of users, roles, and processes to the specific functions and data to which each entity holds authorized access.

11.2.1 – Authorized access
11.2.1-A – Ensuring authorized access
11.2.1-B – Modifying authorized user lists
11.2.1-C – Access control by voting stage
11.2.1-D – Access control configuration
11.2.1-E – Administrator modified permissions
11.2.1-F – Authorized assigning groups or roles
11.2.2 – Role-based access control
11.2.2-A – Role-based access control standard
11.2.2-B – Minimum groups or roles
11.2.2-C – Minimum group or role permissions
11.2.2-D – Applying permissions

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000491

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanisms
- 11.3.1-A – Access control mechanism application
- 11.3.1-B – Multi-factor authentication for critical operations
- 11.3.1-C – Multi-factor authentication for administrators

11.3.2 – User authentication credentials
- 11.3.2-A – Username and password management
- 11.3.2-B – Password complexity
- 11.3.2-C – Secure storage of authentication data
- 11.3.2-D – Password disallow list
- 11.3.2-E – Usernames within passwords

11.4 - The voting system's default access control policies enforce the principles of least privilege and separation of duties.

11.4 – Default access control policies
- 11.4-A – Least privilege for access policies
- 11.4-B – Separation of duties

11.5 - Logical access to voting system assets are revoked when no longer required.

11.5 – Logical access restrictions
- 11.5-A – Session time limits
- 11.5-B – Reauthentication
- 11.5-C – Account lockout
- 11.5-D – Lockout time duration

Principle 12: Physical Security

The voting system prevents or detects attempts to tamper with voting system hardware.

12.1 - The voting system supports mechanisms to detect unauthorized physical access.

12.1 – Mechanisms to detect unauthorized physical access
- 12.1-A – Unauthorized physical access
- 12.1-B – Unauthorized physical access alert
- 12.1-C – Disconnecting a physical device
- 12.1-D – Logging of physical connections and disconnections
- 12.1-E – Secure containers
- 12.1-F – Secure locking systems
- 12.1-G – Backup power for power-reliant countermeasures

12.2 - The voting system only exposes physical ports and access points that are essential to voting operations.

12.2 – Physical ports and access points essential to voting
- 12.2-A – Physical port and access least functionality
- 12.2-B – Physical port auto-disable
- 12.2-C - Physical port restriction
- 12.2-D – Disabling ports
- 12.2-E – Logging enabled and disabled ports

Principle 13: Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1.1 – Configuration file
- 13.1.1-A – Authentication to access configuration file
- 13.1.1-B – Authentication to access configuration file on EMS
- 13.1.1-C – Authentication to access configuration file for network appliances

13.1.2 – Election records
- 13.1.2-A – Integrity protection for election records

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2 – Source and integrity of election records
- 13.2-A – Signing stored election records

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000492

13.2-B – Verification of election records

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.3 – Cryptographic algorithms
13.3-A – Cryptographic module validation
13.3-B – E2E cryptographic voting protocols
13.3-C – Cryptographic strength
13.3-D – MAC cryptographic strength
13.3-E – Cryptographic key management documentation

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

13.4-A – Confidentiality and integrity protection of transmitted data

Principle 14: System Integrity

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.1 – Documented resiliency against security failures and vulnerabilities
14.1-A – Risk assessment documentation
14.1-B – Addressing and accepting risk
14.1-C – System security architecture description
14.1-D – Procedural and operational security

14.2 - The voting system is designed to limit its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2 – Designed to limit attack surface
14.2-A – Non-essential networking interfaces
14.2-B – Network status indicator
14.2-C – Wireless communication restrictions
14.2-D – Wireless network status indicator
14.2-E – External network restrictions
14.2-F – Secure configuration and hardening documentation
14.2-G – Unused code
14.2-H – Use of exploit mitigation technologies
14.2-I – Importing software libraries
14.2-J – Vulnerability management plan
14.2-K – Known vulnerabilities

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3 – Supply chain
14.3-A – Supply chain risk management strategy
14.3-B – Criticality analysis
14.3-C – Bill of materials
14.3.1 – Boot integrity
14.3.1-A – Cryptographic boot verification
14.3.1-B – Preventing of boot on error
14.3.1-C – Notification of boot validation failure
14.3.2 – Software integrity
14.3.2-A – Installing software
14.3.2-B – Software verification for installation
14.3.2-C – Application allowlisting
14.3.2-D – Integrity protection for software allowlists

14.4 - Voting system software updates are authorized by an administrator prior to installation.

14.4 – Authorized software updates

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000493

14.4-A – Authenticated operating system updates

14.4-B – Authenticated application updates
14.4-C – Authenticated firmware updates

Principle 15: Detection and Monitoring

The voting system provides mechanisms to detect anomalous or malicious behavior.

15.1 - Voting system equipment records important activities through event logging mechanisms, which are stored in a format suitable for automated processing.

15.1 – Event logging
15.1-A – Event logging
15.1-B – Exporting logs
15.1-C – Logging voter information
15.1-D – Logging event types
15.1-E – Configuration file access log

15.2 - The voting system generates, stores, and reports all error messages as they occur.

15.2 – Error messages
15.2-A – Presentation of voting application errors
15.2-B – Voting application error handling documentation
15.2-C – Logging system errors
15.2-D – Creating error reports

15.3 - The voting system is designed to protect against malware.

15.3 – Malware protection mechanisms
15.3-A – Malware protection mechanisms
15.3-B – Updatable malware protection mechanisms
15.3-C – Documenting malware protection mechanisms
15.3-D – Notification of malware detection
15.3-E – Logging malware detection
15.3-F – Notification of malware remediation
15.3-G – Logging malware remediation

15.4 - A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practices.

15.4 – Defense against network-based attacks
15.4-A – Internal network architecture documentation
15.4-B – Secure network configuration documentation
15.4-C – Documentation for disabled wireless
15.4-D – Rule and policy updates

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000494

Appendix C References

Reference	Citation
ADA10:	**The Americans with Disabilities Act of 1990.**
ANSI04:	**International Committee for Information Technology Standards, American National Standard for Information Technology – Role Based Access Control (ANSI INCITS 359-2004), February 2004.**
ANSI19:	**American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids, ANSI C63.19-2019.**
ANSI15b:	**CISPR 24:2010+A1:2015, Information technology equipment - Immunity characteristics - Limits and methods of measurement.**
ANSI93:	**ANSI C63.16:1993, American National Standard Guide for Electrostatic Discharge Test – Methodology and Criteria for Electronic Equipment.**
Benaloh14:	**Benaloh et al., End-to-end verifiability, February 2014.**
CA06:	**California Volume Reliability Testing Protocol. January 31, 2006**
CIS20:	**Center for Internet Security, CIS Benchmarks, 2020.**
CVR_CDF:	**Wack et al. Cast Vote Records Common Data Format Specification (NIST SP 1500-103), Version 1.0. February 2019.**
DISA20:	**Defense Information Systems Agency, Security Technical Implementation Guides (STIGs), 2020.**
NIST16:	**Wack et al. Election Results Common Data Format Specification (NIST SP 1500-100), Version 2.0, September 2019.**
FCC18:	**FCC regulations for hearing aids, 47 CFR Parts 20 and 68: Hearing Aid Standard, includes useful information about how to test audio volume and quality.**
FCC19a:	**Title 47, Part 15, Rules and Regulations of the Federal Communications Commission, Radio Frequency Devices.**
GPO19:	**Government Paper Specification Standards No. 13, May 2019.**
HAVA02:	**The Help America Vote Act of 2002, Public Law 107-252.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000495

ISO00:	**ISO/IEC TR 15942:2000, Information technology—Programming languages—Guide for the use of the Ada programming language in high integrity systems.**
ISO06b:	**ISO/IEC 25062:2006 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability Test Reports.**
ISO10:	**ISO/IEC TR 25060:2010** **Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: General framework for usability-related information.**
ISO13a:	**ISO/IEC TR 24772:2013** **INFORMATION TECHNOLOGY -- PROGRAMMING LANGUAGES -- GUIDANCE TO AVOIDING VULNERABILITIES IN PROGRAMMING LANGUAGES THROUGH LANGUAGE SELECTION AND USE.**
ISO13b:	**ISO/IEC 25064:2013** **Systems and software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability: User needs report.**
ISO14:	**ISO/IEC 25063:2014** **Systems and software engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for usability:**
ISO16:	**ISO/IEC 25066:2016 Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Evaluation report**
ISO18:	**ISO/IEC/IEEE 90003:2018** **SOFTWARE ENGINEERING -- GUIDELINES FOR THE APPLICATION OF ISO 9001:2015 TO COMPUTER SOFTWARE.**
ISO18d:	**ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management, July 2017.**
ISO19a:	**ISO/IEC PRF TR 24772-1** **PROGRAMMING LANGUAGES -- GUIDANCE TO AVOIDING VULNERABILITIES IN PROGRAMMING LANGUAGES -- PART 1: LANGUAGE INDEPENDENT.**
ISO19b:	**ISO/IEC 9294-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.**
ISO8601	**ISO/IEC 8601-1:2019 Date and Time Format.**
ITU19:	**International Telecommunications Union (ITU) (nd) Rec. ITU-T P.50 October 2019.**
Kulyk18:	**Oksana Kulyk, Melanie Volkamer, Usability is not Enough: Lessons Learned from 'Human Factors in Security' Research for Verifiability, October 2018.**

AMERICAN OVERSIGHT

Lewis19a:	**Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague, *Ceci n'est pas une preuve*, March 2019.**
Lewis19b:	**Sarah Jamie Lewis, Olivier Pereira, Vanessa Teague, How not to prove your election outcome, March 2019.**
LOG_CDF:	**Wack et al. Election Event Logging Common Data Format Specification Draft (NIST SP 1500-101), Version 1.0. September 2017.**
MITRE20:	**MITRE Common Weakness Enumeration 561: Dead Code, August 2020.**
MITRE20a:	**MITRE Common Weakness Enumeration 259: Use of Hard-coded Password, August 2020.**
MITRE20b:	**MITRE Common Weakness Enumeration 321: Use of Hard-coded Cryptographic Key, August 2020.**
MITRE20c:	**MITRE Common Weakness Enumeration 116: Improper Encoding or Escaping of Output, June 2020.**
MITRE20d:	**MITRE Common Weakness Enumeration 134: Use of Externally-Controlled Format String, August 2020.**
MITRE20e:	**MITRE Common Weakness Enumeration 89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), August 2020.**
Moulding89:	**M. R. Moulding, "Designing for high integrity: the software fault tolerance approach," Section 3.4. In C. T. Sennett, ed., High-Integrity Software, Plenum Press, New York and London, 1989.**
NIST01:	**National Institute of Standards and Technology Federal Information Processing Standards 140-2: Security Requirements for Cryptographic Modules, May 2001.**
NIST07:	**Karen Scarfone, Peter Mell, National Institute of Standards and Technology Special Publication 800-94: Guide to Intrusion Detection and Prevention Systems, February 2007.**
NIST08:	**Dana E. Chisnell, Susan C. Becker, Sharon J. Laskowski, Svetlana Z. Lowry, National Institute of Standards and Technology IR 7519, Style Guide for Voting System Documentation, August 2008.**
NIST09:	**Karen Scarfone and Paul Hoffman, National Institute of Standards and Technology Special Publication 800-41, Revision 1: Guidelines on Firewalls and Firewall Policy, September 2009.**
NIST09a:	**Janice (Ginny) Redish and Sharon J. Laskowski, National Institute of Standards and Technology IR 7596, Guidelines for Writing Clear Instructions and Messages for Voters and Poll Workers, May 2009.**
NIST12:	**Joint Task Force Transformation Initiative, National Institute of Standards and Technology Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments, September 2012.**
NIST13a:	**Murugiah Souppaya, Karen Scarfone, National Institute of Standards and Technology Special Publication 800-83, Revision 1: Guide to Malware Incident Prevention and Handling for Desktops and Laptops, July 2013.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000497

NIST13b:	**Murugiah Souppaya, Karen Scarfone, National Institute of Standards and Technology Special Publication 800-40, Revision 3: Guide to Enterprise Patch Management Technologies, July 2013.**
NIST13c:	**National Institute of Standards and Technology Federal Information Processing Standards 186-4: Digital Signature Standard, July 2013.**
NIST15a:	**Elaine Barker, John Kelsey, National Institute of Standards and Technology Special Publication 800-90A, Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015.**
NIST15b:	**Jon Boyens et al., National Institute of Standards and Technology Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015**
NIST17c:	**Paul A. Grassi, Michael E. Garcia, James L. Fenton, National Institute of Standards and Technology Special Publication 800-63-3: Digital Identity Guidelines, June 2017.**
NIST17d:	**Paul A. Grassi et al., National Institute of Standards and Technology Special Publication 800-63B: Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017.**
NIST17e:	**Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri, National Institute of Standards and Technology Special Publication 800-12, Revision 1: An Introduction to Information Security, June 2017.**
NIST18a:	**Turan et al. National Institute of Standards and Technology Special Publication 800-90B: Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018.**
NIST18b:	**Celia Paulsen, Jon Boyens, Nadya Bartol, Kris Winkler, National Institute of Standards and Technology Interagency or Internal Report 8179: Criticality Analysis Process Model: Prioritizing Systems and Components, April 2018.**
NIST18c:	**National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018.**
NIST19a:	**National Institute of Standards and Technology Federal Information Processing Standards 140-3: Security Requirements for Cryptographic Modules, March 2019.**
NIST19b:	**Kerry McKay, David Cooper, National Institute of Standards and Technology Special Publication 800-52, Revision 2: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, August 2019.**
NIST20a:	**Eliane Barker, National Institute of Standards and Technology Special Publication 800-57 Part 1, Revision 5: Recommendation for Key Management Part 1 – General, May 2020.**
NIST20b:	**Joint Task Force, National Institute of Standards and Technology Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations, September 2020.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000498

NIST20c:	**Kelley Dempsey, Eduardo Takamura, Paul Eavy, George Moore, National Institute of Standards and Technology Interagency or Internal Report 8011 Volume 4: Automation Support for Security Control Assessments: Software Vulnerability Management, April 2020.**
NIST20d:	**Celia Paulsen et al., National Institute of Standards and Technology Interagency or Internal Report 8272: Impact Analysis Tool for Interdependent Cyber Supply Chain Risks, August 2020**
NIST20e:	**National Institute of Standards and Technology Cryptographic Module Validation Program, October 2020.**
NIST20f:	**Elaine Barker, Allen Roginsky, Richard Davis, National Institute of Standards and Technology Special Publication 800-133, Revision 2: Recommendation for Cryptographic Key Generation, June 2020.**
NIST20g:	**Elaine Barker, National Institute of Standards and Technology Special Publication 800-175B, Revision 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, March 2020.**
NIST20h:	**Security and Privacy Controls for Information Systems and Organizations, National Institute of Standards and Technology Special Publication 800-53, Revision 5, September 2020.**
NTIA19:	**National Telecommunications and Information Administration, Software Bill of Materials, 2019.**
OCD-ID:	**Open Civic Data Identifiers Specification.**
OWASP19:	**Open Web Application Security Project, Application Security Verification Standard 4.0, March 2019.**
Rivest06:	**Ronald R. Rivest and John P. Wack, "On the notion of "software independence" in voting systems," July 28, 2006.**
SAFECode19:	**SAFECode, Managing Security Risks Inherent in the Use of Third-party Components, May 2019.**
TC04:	**Trace Center (2004), About Decibels (dB).**
TCnd:	**Trace Center (nd). EZ Access design is an example of button functions distinguishable by both shape and color.**
UL07:	**UL 60950-1:2007, Edition 2, Information Technology Equipment – Safety – Part 1: General Requirements. March 27, 2007.**
UL13:	**UL 437:2013, Edition 8, Standard for Key Locks. May 15, 2013.**
UL19:	**UL 62368:1 Edition 3, Standard for Audio/video, Information and Communication Technology Equipment - Part 1: Safety requirements**
USAB14a:	**US Access Board Technical Guide: Clear Floor or Ground Space and Turning Space. February 2014.**
USAB14b:	**US Access Board Guide to the ADA Standards, Chapter 3 Operable Parts.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000499

USAB18:	**US Access Board (2018) Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines (36 CFR Parts 1193 and 1194, RIN 3014-AA37, Final Rule, March 23, 2018)**
USDOJ16:	**US Department of Justice ADA Checklist for Polling Places, 2016.**
VRA65:	**The Voting Rights Act of 1965, Public Law 89-110, August 6, 1965.**
VRI_CDF:	**Wack et al. Voter Records Interchange (VRI) CDF Specification (NIST SP 1500-102), Version 1.0. August 2017.**
VSS1990:	**Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, January 1990 edition with April 1990 revisions, in Voting System Standards, U.S. Government Printing Office, 1990.**
VVSG2005:	**2005 Voluntary Voting System Guidelines, Version 1.0, Volumes I and II, March 6, 2006.**
VVSG2015:	**2015 Voluntary Voting System Guidelines, Version 1.1, Volumes I and II. March 31, 2015.**
W3C10:	**W3C WAI (2010) WCAG 2.0 Web content and Accessibility Guidelines.**

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000500

From: Pauley, Scott <Scott.Pauley@sos.mo.gov>
To: TiffanyEllison@claycoelections.com
pattylamb@claycoelections.com
Date: 12/16/2022 10:57:16 AM
Subject: Recount - State Representative, District 17
Attachments: 1. Memo to LEA - Clay.docx
2. House District 17 Notice of Recount.pdf
3. Recount Instructions for November 2022.docx
4. Schedule for Recount to send to LEA.docx
5. Oath - Sworn Statement.pdf
6. Tally Summary Sheet Dist 17.doc
7. Report of Findings Dist 17.doc
8. Recount Checklist.docx
9a. 15c30-9.pdf
9b. 15c30-10.pdf
10. Dolan v Powers 260_S.W.3d_376.pdf

Good morning,

You will find attached to this email information relating to the recount for the office of State Representative, District 17. We are also notifying the candidates of the recount request today and will provide their lists of disinterested individuals to you once we receive them.

The attached instructions (Item 3) list the steps to be taken during the recount process and the deadlines for each to be completed. In accordance with those deadlines, please complete the Schedule for Recount (Item 4) and return the date /time of the recount to our office no later than 10 a.m. on Monday, December 19, so we may share this with the candidates and their legal counsel.

If you have any questions or concerns during this process, please feel free to contact our office.

Elections Division
Missouri Secretary of State
T: 573-751-2301/800-669-8683
elections@sos.mo.gov

AMERICAN OVERSIGHT

JOHN R. ASHCROFT
SECRETARY OF STATE
STATE OF MISSOURI

JAMES C. KIRKPATRICK
STATE INFORMATION CENTER
(573) 751-4936

ELECTIONS DIVISION
(573) 751-2301

MEMO

TO: Tiffany Ellison and Patty Lamb, Directors, Clay County Board of Elections

FROM: Chrissy Peters, Director of Elections

DATE: December 16, 2022

RE: Notification of Recount

Enclosed is the official Notification of Recount and related documents for conducting the recount of State Representative, District 17:

1. Notification of Recount
2. Recount procedures and timeline
3. Schedule for recount
4. Oath for Judges
5. Tally summary sheet
6. Report of findings
7. Recount checklist
8. Rules 15 CSR 30-9; 15 CSR 30-10.010, 10.040, 10.140
9. *Dolan v. Powers*

Should you have any questions regarding these materials, please call our office at (800) 669-8683.

Enclosures

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000502

STATE OF MISSOURI

Office of
Secretary of State

NOTIFICATION OF RECOUNT
Pursuant to Section 115.601.3, RSMo.

THE MISSOURI SECRETARY OF STATE,

To the Clay County Board of Elections:

WHEREAS, I have been duly notified that the results of the General Election November 8, 2022, for the Office of State Representative District 17, established the defeat of one candidate by less than one-half of one percent of the votes cast; and

WHEREAS, I have been requested by Mark Ellebracht, the candidate who received the lowest number of votes and was defeated by less than one-half of one percent of the votes cast, to hold a recount of the votes in the race for State Representative, District 17, pursuant to Section 115.601, RSMo.

NOW THEREFORE, I, JOHN R. ASHCROFT, SECRETARY OF STATE OF MISSOURI, do hereby issue this Notification of Recount to the Clay County Board of Elections and further authorize the Clay County Board of Elections to recount the ballots in its jurisdiction during the November 8, 2022, General Election for the Office of State Representative, District 17. The recount of ballots in this jurisdiction shall be conducted according to procedures directed by the Secretary of State. The Clay County Board of Elections shall certify and deliver results of this recount to the Secretary of State's Office on or before January 3, 2023.

SEAL OF THE SECRETARY OF STATE
MISSOURI

IN TESTIMONY WHEREOF, I hereunto set my hand and affix the Seal of my office. Done at the City of Jefferson, this 16th day of December, 2022.

Jay Ashcroft

Secretary of State

AMERICAN OVERSIGHT

Missouri Secretary of State
November 8, 2022 General Election – State Representative, District 17
Official Recount Procedures and Timeline

The recount of the November 8, 2022, General Election for the office of State Representative, District 17 will be conducted under the following timeline and procedures established by the Missouri Secretary of State's Office in accordance with Section 115.601, RSMo.

This comprehensive recount is designed to ensure that the final results are complete, accurate and reflect the intent of every voter. To do this, every ballot should be manually reviewed as set forth in these procedures. You will note that these recount procedures provide for a combination of human review, electronic counting, and hand tallying to ensure the most accurate, efficient, and fair recount possible.

Timeline

Activity	Deadline
SOS notifies and sends procedures to LEAs and the concerned parties (Candidates, highest vote and second highest vote)	12/16/22
LEAs return recount date, time, and place to SOS	12/19/22 by 10:00 AM
SOS notifies the concerned parties of the LEAs' scheduled recount date, time, and place	12/19/22
Concerned parties provide disinterested person lists to SOS	12/23/22
SOS sends lists of disinterested persons to LEAs	12/27/22
Recount begins (LEAs must choose disinterested persons at least one day before recount)	After 12/27/22
LEA deadline for return of certified findings to SOS	1/3/23
SOS certifies recount results	1/4/23

Procedures

Step 1: Recount Request
If a recount request is received prior to certification, such recount will be considered to be effective the day the election results are certified in accordance with Chapter 115, RSMo. Section 115.601, RSMo., requires all recount requests to be filed no later than seven days after certification of the election. If a request is received before the deadline, the recount can begin immediately after certification.

Step 2: Selection and notification of disinterested persons
Disinterested persons are defined in Section 115.601, RSMo. The concerned parties provide to the Secretary of State a list of individuals to observe the recount. Missouri law requires these individuals to be a disinterested person and a registered voter of the area where the contested election was held. A disinterested person may only observe the recount taking place in the jurisdiction in which he or she is registered to vote.

AMERICAN OVERSIGHT

The Secretary of State's office delivers each party's list to the LEA. The LEA will work with the concerned parties to use the list provided by the SOS to ensure that only two of the named individuals from each party's list serves as disinterested persons. LEAs must choose disinterested persons at least one day before their recount begins. Participating disinterested persons observe the recount and sign the LEA's Report of Findings. Concerned parties are not required to provide disinterested persons in every or any jurisdiction.

Step 3: Administration of Recount

1. Only LEA, LEA staff, bipartisan teams of election judges, the appointed disinterested persons (four total), the concerned parties (or their attorneys), and if requested, a representative from the Secretary of State's Office may be present during the recount.

2. The LEA must swear in, using the form provided, each participant identified in #1 above.

3. All election judges and disinterested persons must receive the same pay as an election judge in the jurisdiction where the person is registered.

4. No documents or copies of documents, other than the Report of Findings to the Secretary of State's Office, can be released to anyone present at the recount, although the concerned parties and disinterested persons may receive copies of the oaths they execute. (Section 115.601.4, RSMo.)

5. The LEA shall make arrangements for media, if requested, to be allowed to view the recount procedures. Although state law does not allow media to be present in the room where the recount is occurring, the LEA's recount process should be as transparent as practical. For example, the recount process could be conducted in a conference room that contains windows and conducted in a manner where the media could observe the process overall but not the identifiable information and/or marked ballots.

Step 4: Ballot Counting

For the purpose of these procedures, a recount is one additional counting of all votes counted in the November 8, 2022, general election for the office of State Representative, District 17.

Ballot counting – optical scan

Only the LEA, LEA staff, and the bipartisan teams of election judges can conduct the recount; no additional assistance can be provided by other parties. Concerned parties and disinterested persons may observe, but may not handle the ballots. If present, representatives from the Secretary of State's Office are not permitted to make a determination on how a ballot should be counted.

1. After all participants have taken their oath, the LEA will conduct a test of the voting equipment to be used in the recount. The test deck must consist of General Election ballots that are marked as follows and totaling at least ten ballots:

   - 4 votes for Bill Allen
   - 3 votes for Mark Ellebracht
   - 1 with no votes for any State Representative, District 17 candidates (undervoted)
   - 1 with votes for two State Representative, District 17 candidates (overvoted)

Refer to 15 CSR 30-10.040 and 15 CSR 30-10.140 (copy enclosed).

AMERICAN OVERSIGHT

2. The LEA breaks the seal on ballots.

3. Only ballots with votes for State Representative, District 17 candidates can be counted. The bipartisan team of election judges must sort the ballots as below. The team must follow the current counting standards (15 CSR 30-9.020). See also *Dolan v. Powers,* 260 S.W.3d 376 (Mo. App. W.D. 2008). Ballots containing marks in or around the candidate names constitute a distinguishing mark.

   The bipartisan team of election judges must sort the ballots as below.
   - Group A: General Election ballots with distinguishing marks in the designated area for State Representative, District 17 candidates (this does not include undervotes or overvotes).
   - Group B: General Election ballots without distinguishing marks or with marks outside designated area for State Representative, District 17 candidates (this does include undervotes and overvotes).

4. For the Group A ballots, perform the following:

   a. Prepare for counting these ballots through the LEA's optical scan tabulating machine.

   b. During this process, participants will also be watching for any distinguishing mark of voter intent in accordance with the current counting standards (15 CSR 30-9.020 and *Dolan v. Powers*, 260 S.W.3d 376 (Mo. App. W.D. 2008)), a copy of which is enclosed. If any are identified, follow step 5 below.

   c. The bipartisan team of election judges, under the observation of the disinterested persons, feeds the Group A ballots *face up* into the counting machine(s).

   d. The bipartisan team of election judges will record the total votes on the LEA's tally summary sheet (form provided) and incorporate these into the Report of Findings.

5. For the Group B ballots, perform the following:

   a. The bipartisan team of election judges, observed by the disinterested persons will review the ballots again to determine if there is any distinguishing mark of voter intent, following the current counting standards (15 CSR 30-9.020). See also *Dolan v. Powers*, 260 S.W.3d 376 (Mo. App. W.D. 2008). Ballots containing marks in or around any State Representative, District 17 constitute a distinguishing mark.

   b. For those ballots determined to show voter intent, the bipartisan team of election judges will record those total votes on the LEA's tally summary sheet (form provided) and incorporate these into the Report of Findings.

6. After the electronic recount is completed, the LEA must run a post test of the voting equipment using the test deck used in Step 1.

AMERICAN OVERSIGHT

Ballot counting – DREs

NOTE: This process was modified in 2015, as requested by the local election authorities.

Only the LEA, LEA staff, and the bipartisan teams of election judges can conduct the recount; no additional assistance can be provided by other parties. Concerned parties and disinterested persons may observe, but may not handle the paper trails, containers, and DREs. If present, the representative from the Secretary of State's Office are not permitted to make a determination on how a ballot should be counted.

1. The LEA breaks the seal on the DRE component that contains the summary of all votes cast.

2. The bipartisan team of election judges examines the summary of all votes cast in the State Representative, District 17, records the totals on the LEA's tally summary sheet (form provided) and incorporates the totals into the Report of Findings.

3. If the summary of all votes cast is not usable for the recount, the LEA will use the audit trail* from each DRE that was created contemporaneously with the voter verified paper trail (*as defined in 15 CSR 30-10.010), and hand tally each ballot. The LEA must then separately seal and secure the DRE component for possible further inspection.

Step 5: Report of Findings

1. The bipartisan team of election judges records the total result from the tally summary sheet onto the Report of Findings.

2. The disinterested persons present must sign the Report of Findings, along with the LEA. If disinterested persons are not present for the recount, the LEA is the only signer of the Report of Findings.

Step 6: Transmit to SOS

The LEA must return the following forms to the SOS no later than seven days after recount begins.

1. Report of Findings (enclosed)
2. Administered oaths (enclosed)
3. Tally summary sheet (enclosed)

The LEA must also keep copies of all originals of these documents in their office.

Exception to Procedures

The above procedures apply except as otherwise agreed to by the concerned parties and approved by the LEA and the SOS. Any proposed exceptions to these procedures must be signed by each concerned party and the LEA and submitted to the SOS in writing no later than 5:00 p.m. on December 23, 2022.

Requests for Secretary of State Observers

The concerned parties or LEAs may request that staff from the Secretary of State's office observe a recount occurring in a particular jurisdiction(s). Any requests must specify the jurisdiction and be submitted to the SOS in writing (sent to elections@sos.mo.gov or by letter at 600 W. Main St., Jefferson City, MO 65101) no later than 5:00 p.m. on December 23, 2022. This is subject to staff availability of the SOS.

AMERICAN OVERSIGHT

Schedule for Recount
State Representative, District 17
November 8, 2022, General Election

_____
County/Jurisdiction

will conduct its recount on

_____
Date
(No earlier than 12/27/2022)

_____
Time

_____
Location

_____
Signature of Election Authority

FAX/EMAIL BACK IMMEDIATELY TO
Missouri Secretary of State's Office

573-526-3242
Elections@sos.mo.gov

AMERICAN OVERSIGHT

I solemnly swear that I will impartially discharge the duties of judge according to law, to the best of my ability and that I will not disclose how any voter has voted unless I am required to do so as a witness in a proper judicial proceeding. I also affirm that I will not allow any person to vote who is not entitled to vote and that I will make no statement nor give any information of any kind tending in any way to show the state of the count prior to the close of the polls on election day.

I further swear that I will not disclose any facts uncovered by the recount, except those which are contained in the Report of Findings.

Sworn and subscribed to before me this .....day of ....., 20.....

.....
Judge of Election

.....
Election Authority (Judge of Election) witnessing oath

AMERICAN OVERSIGHT

Tally Summary Sheet

_____

Local Election Authority Name

Optical Scan Summary	**Electronic**	**Manual**
Group A - Number of General Election ballots with distinguishing marks in the designated area for State Representative, District 17 candidates (this does not include undervotes or overvotes).		
Group B – Number of General Election ballots without distinguishing marks or with marks outside designated area for State Representative, District 17 candidates (this does include undervotes and overvotes)		
Total of Group A and B		

DRE Summary	**Count**
The summary of all votes cast for State Representative, District 17 candidates.	

Candidate	**O/S electronic recount totals**	**O/S manual recount totals**	**DRE manual recount totals**	**Totals**
Bill Allen				
Mark Ellebracht				

AMERICAN OVERSIGHT

Report of Findings
State Representative, District 17 of November 8, 2022, Election

_____
County/Jurisdiction

_____
Name of Local Election Authority

We the undersigned hereby certify that the recount conducted of the State Representative, District 17 General Election revealed the number of votes cast for each candidate was as follows:

Number of Votes

Bill Allen _____

Mark Ellebracht _____

Disinterested persons assisting (please list first and last name of each disinterested person):

_____ _____
Name Signature

_____ _____
Name Signature

_____ _____
Name Signature

_____ _____
Name Signature

_____
Local Election Authority Signature

_____
Date of Signature

AMERICAN OVERSIGHT

Local Election Authority
Recount Checklist

_____ Lock door(s) to counting room

_____ Note all persons in attendance (No unauthorized persons in attendance)

_____ County Clerk/Election Authority swears in all attendees, reminding attendees they are not allowed to disclose any details from this recount

_____ County Clerk/Election Authority removes ballots from sealed/secured location

_____ Recount begins

_____ County Clerk/Election Authority seals/secures ballots

_____ Complete *Report of Findings*

_____ Obtain signatures on *Report of Findings*

_____ County Clerk/Election Authority signs and certifies results

_____ Door(s) may be unlocked

AMERICAN OVERSIGHT

Rules of
Elected Officials
Division 30—Secretary of State
Chapter 9—Uniform Counting Standards

Title		Page
15 CSR 30-9.010	Uniform Counting Standards—Punch Card Voting Systems	3
15 CSR 30-9.020	Uniform Counting Standards—Optical Scan Voting Systems	3
15 CSR 30-9.030	Uniform Counting Standards—Paper Ballots	5
15 CSR 30-9.040	Write-In Stickers	7

AMERICAN OVERSIGHT

Title 15—ELECTED OFFICIALS
Division 30—Secretary of State
Chapter 9—Uniform Counting Standards

15 CSR 30-9.010 Uniform Counting Standards—Punch Card Voting Systems

PURPOSE: This rule provides for standards to be used by election authorities when counting ballots cast using punch card voting systems.

(1) The election authority shall be responsible for insuring that the standards provided for in this rule are followed when counting ballots cast using punch card voting systems.

(2) Prior to tabulating ballots, all ballot cards shall be inspected by the election authority for hanging chad and/or damaged ballots.

(3) Inspection of ballot cards shall be conducted using the following guidelines:

(A) The election authority shall appoint a bipartisan team to inspect all ballots where a question exists about the condition of a ballot or existence of hanging chad;

(B) All ballot card inspections conducted pursuant to this section shall be conducted by examining the ballot card from the back of the card;

(C) If a ballot is determined to be damaged, the bipartisan team shall spoil the original ballot and duplicate the voter's intent on the new ballot, provided that there is an undisputed method of matching the duplicate card with its original after it has been placed with the remainder of the ballot cards from that precinct; and

(D) If a chad is determined to be hanging by two (2) or less corners, it shall be removed prior to being tabulated.

(4) In jurisdictions using punch card systems, a valid vote for a write-in candidate must include the following:

(A) A distinguishing mark in the square immediately preceding the name of the candidate;

(B) The name of the candidate. If the name of the candidate, as written by the voter, is substantially as declared by the candidate it shall be counted, or in those circumstances where the names of candidates are similar, the names of candidates as shown on voter registration records shall be counted; and

(C) The name of the office for which the candidate is to be elected.

(5) Whenever a hand recount of votes is ordered of punch card ballots, the provisions of this section shall be used to determine voter intent.

AUTHORITY: section 115.225, RSMo 2000. Original rule filed Aug. 8, 2001, effective March 1, 2002.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995.*

15 CSR 30-9.020 Uniform Counting Standards—Optical Scan Voting Systems

PURPOSE: This rule provides for standards to be used by election authorities when counting ballots cast using optical scan voting systems.

(1) The election authority shall be responsible for insuring that the standards provided for in this rule are followed when counting ballots cast using optical scan voting systems.

(2) Prior to tabulating ballots all machines shall be programmed to reject blank ballots where no votes are recorded, or where an overvote is registered in any race.

(A) In jurisdictions using precinct-based tabulators, the voter who cast the ballot shall review the ballot if rejected, to determine if he/she wishes to make any changes to the ballot or if he/she would like to spoil their ballot and receive another ballot.

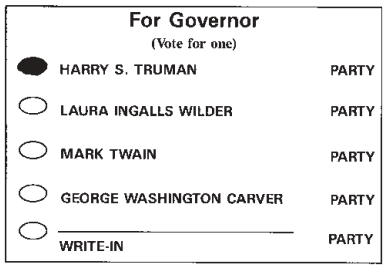
(B) In jurisdictions using centrally-based tabulators, if a ballot is so rejected, it shall be reviewed by a bipartisan team using the following criteria:

1. If a ballot is determined to be damaged, the bipartisan team shall spoil the original ballot and duplicate the voter's intent on the new ballot, provided that there is an undisputed method of matching the duplicate card with its original after it has been placed with the remainder of the ballot cards from that precinct; and

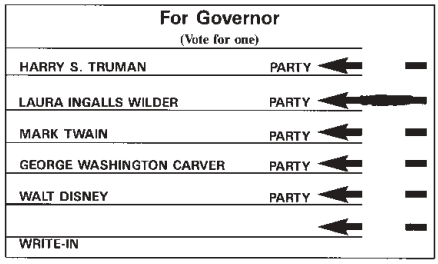
2. The provisions of sections (3), (4), (5) and (6) of this rule.

(3) The following marks shall be considered expressions of voter intent:

(A) Any ballot which is properly marked in the target area, as specified by the ballot instructions.



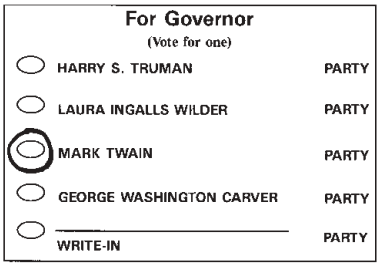
This constitutes a vote for Harry S. Truman.



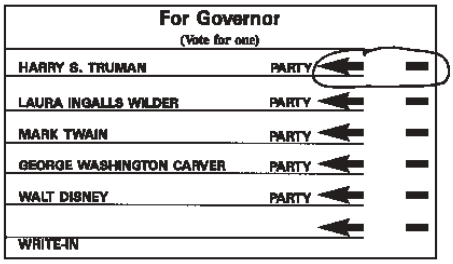
This constitutes a vote for Laura Ingalls Wilder.

(B) Any ballot that is properly marked with any device other than the approved marking device which prevents a machine count shall be counted as a vote.

(C) The target area next to a candidate or issue preference is circled.

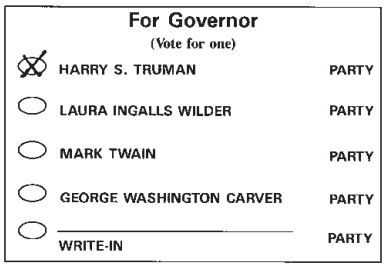


This constitutes a vote for Mark Twain.

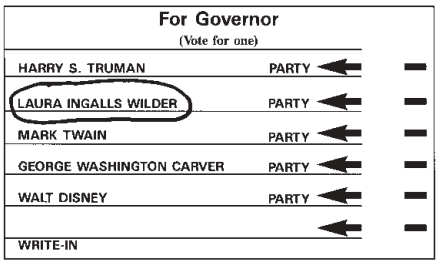


This constitutes a vote for Harry S. Truman.

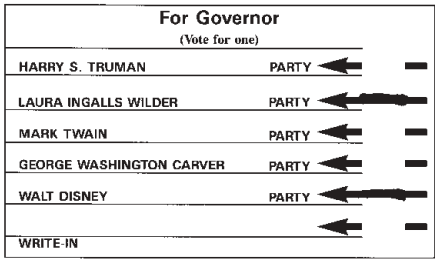
(D) There is a distinguishing mark in the target area next to a candidate or issue preference including but not limited to the following examples:



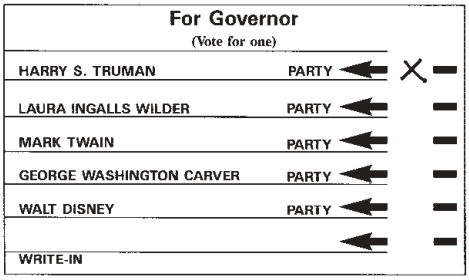
This constitutes a vote for Harry S. Truman.



This constitutes a vote for Laura Ingalls Wilder.

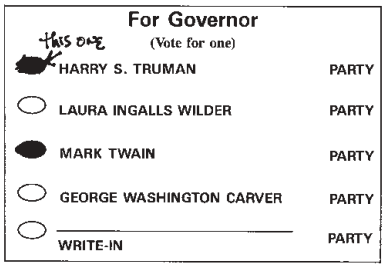


This constitutes an overvote.

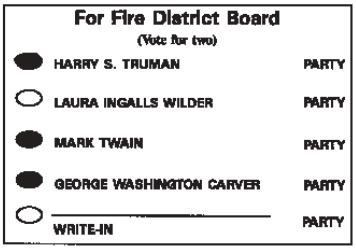


This constitutes a vote for Harry S. Truman.

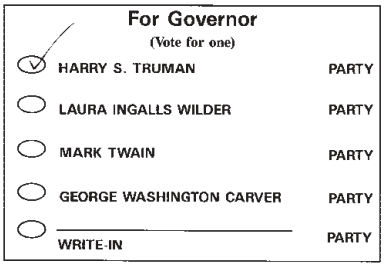
(F) In the event that there are distinguishing marks for two (2) or more candidates, clarified by an additional mark or marks that appear to indicate support, the ballot shall be counted as a vote for the candidate with the additional, clarifying marks.



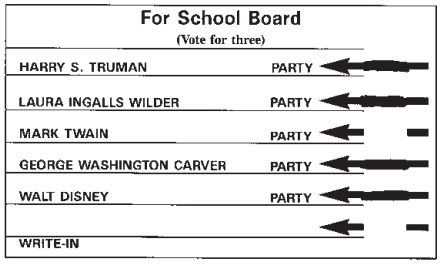
This constitutes a vote for Harry S. Truman.



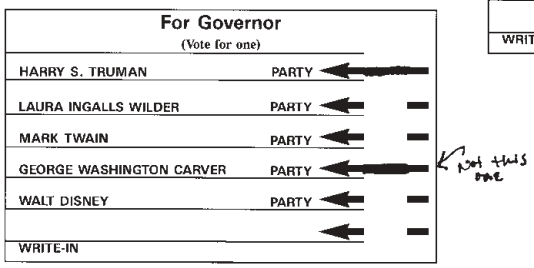
This constitutes an overvote.



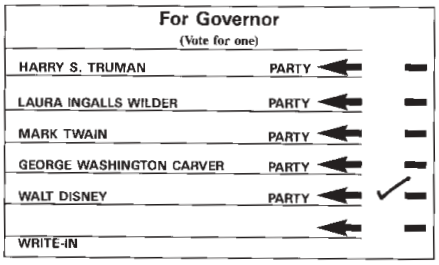
This constitutes a vote for Harry S. Truman.



This constitutes an overvote.

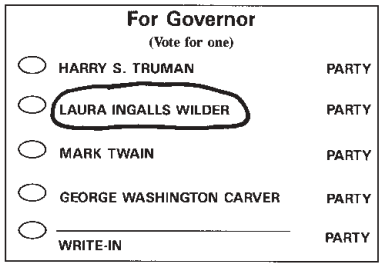


This constitutes a vote for Harry S. Truman.



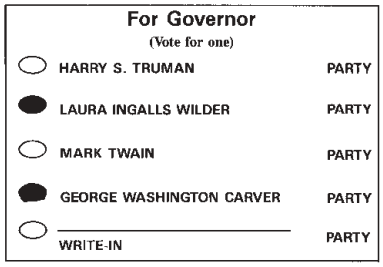
This constitutes a vote for Walt Disney.

(E) The name of a candidate or issue preference is circled.



This constitutes a vote for Laura Ingalls Wilder.

(4) If a voter marks more candidates than there are positions to be elected for that office, without any additional clarifying marks, the marks do not constitute a valid vote for any candidate in that race and the ballot shall be deemed an overvote.



This constitutes an overvote.

(5) In jurisdictions using optical scan systems, a valid vote for a write-in candidate must include the following:

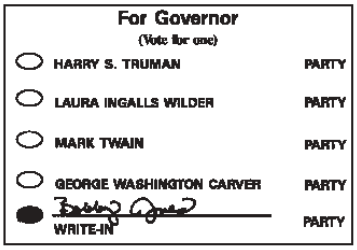
(A) A distinguishing mark in the target area next to the name of the candidate;

(B) The name of a qualified write-in candidate. If the name of the candidate, as written by the voter, is substantially as declared by the candidate it shall be counted, or in those circumstances where the names of candidates are similar, the names of candidates as shown on voter registration records shall be counted; and

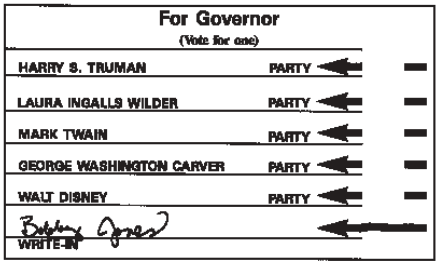
(C) The name of the office for which the candidate is to be elected.

AMERICAN OVERSIGHT

MO-SOS-23-091-A-000515



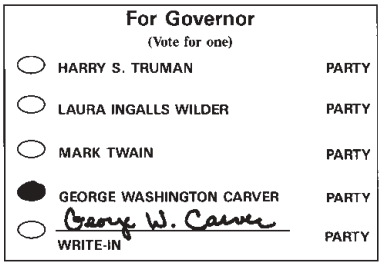
Bobby Jones is a qualified candidate. This constitutes a vote for Bobby Jones.



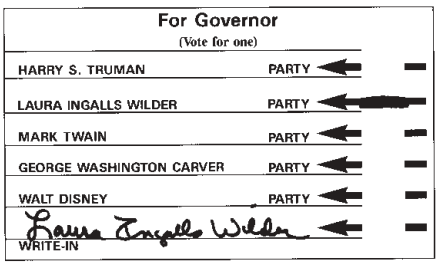
Bobby Jones is a qualified candidate. This constitutes a vote for Bobby Jones.

(6) If a voter designates a vote for a named candidate on the ballot and also provides for a write-in candidate in the same race it shall be treated as follows:

(A) If a voter designates a vote for a named candidate on the ballot and writes in the same candidate in the write-in area, the vote shall count for that candidate.

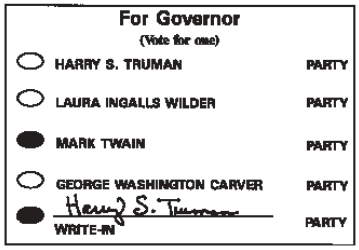


This constitutes a vote for George Washington Carver.

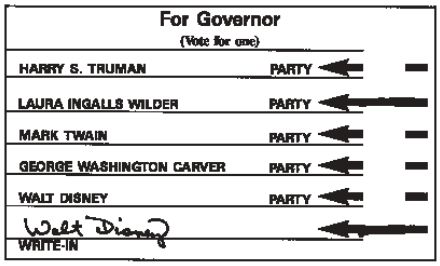


This constitutes a vote for Laura Ingalls Wilder.

(B) If a voter designates a vote for a named candidate on the ballot and writes in the name of a qualified write-in candidate or the name of a different named candidate on the ballot in that race and makes a distinguishing mark in the target area next to the name of the write-in candidate, it shall be considered an overvote with neither candidate receiving credit for the vote.

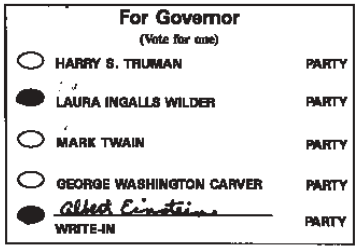


This constitutes an overvote.

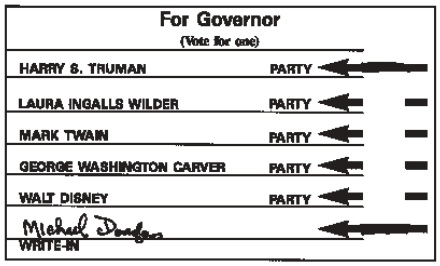


This constitutes an overvote.

(C) If a voter designates a vote for a named candidate on the ballot and writes in the name of a person who is not a qualified write-in candidate and not a named candidate on the ballot in that race, it shall be considered a vote for the named candidate.



Albert Einstein is not a qualified candidate. This constitutes a vote for Laura Ingalls Wilder.



Michael Douglas is not a qualified candidate. This constitutes a vote for Harry S. Truman.

(7) Whenever a hand recount of votes of optical scan ballots is ordered, the provisions of this rule shall be used to determine voter intent.

AUTHORITY: section 115.225, RSMo Supp. 2005. Original rule filed Aug. 8, 2001, effective March 1, 2002. Emergency rescission filed Feb. 2, 2006, effective Feb. 18, 2006, expired Aug. 16, 2006. Emergency rule filed Feb. 2, 2006, effective Feb. 18, 2006, terminated April 30, 2006. Emergency rule filed April 20, 2006, effective April 30, 2006, expired Aug. 16, 2006. Rescinded and readopted: Filed Feb. 2, 2006, effective July 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

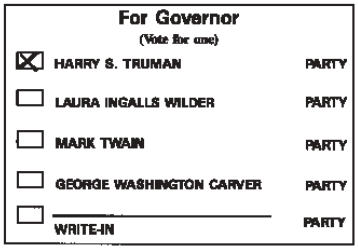
15 CSR 30-9.030 Uniform Counting Standards—Paper Ballots

PURPOSE: This rule provides for standards to be used by election authorities when counting ballots cast using paper ballots.

(1) The election authority shall be responsible for insuring that the standards provided for in this rule are followed when counting ballots cast using paper ballots.

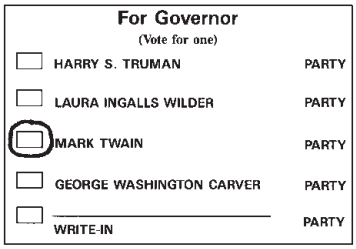
(2) The following marks shall be considered expressions of voter intent:

(A) Any ballot which is properly marked, as specified by the ballot instructions, in the target area.



This constitutes a vote for Harry S. Truman.

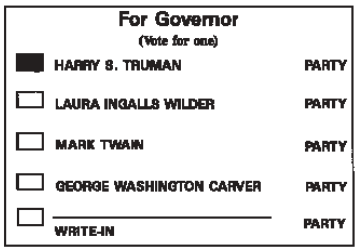
(B) The target area next to a candidate or issue preference is circled.



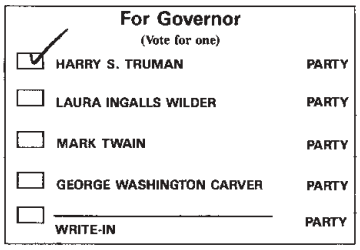
This constitutes a vote for Mark Twain.

(C) There is a distinguishing mark in the target area next to a candidate or issue preference including but not limited to the following examples:

AMERICAN OVERSIGHT

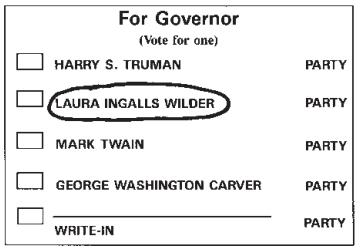


This constitutes a vote for Harry S. Truman.



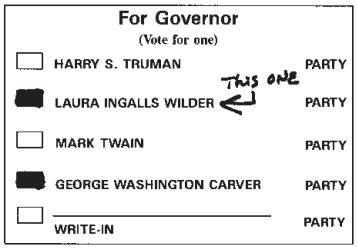
This constitutes a vote for Harry S. Truman.

(D) The name of a candidate or issue preference is circled.



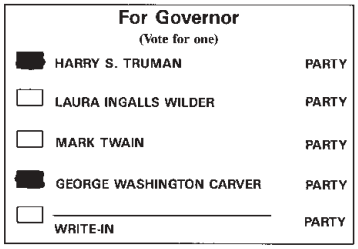
This constitutes a vote for Laura Ingalls Wilder.

(E) In the event that there are distinguishing marks for two (2) or more candidates, clarified by an additional mark or marks that appear to indicate support, the ballot shall be counted as a vote for the candidate with the additional, clarifying marks.

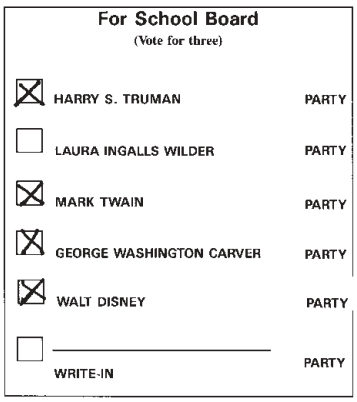


This constitutes a vote for Laura Ingalls Wilder.

(3) If a voter marks more candidates than there are positions to be elected for that office, without any additional clarifying marks, the marks do not constitute a valid vote for any candidate in that race and the ballot shall be deemed an overvote.



This constitutes an overvote.



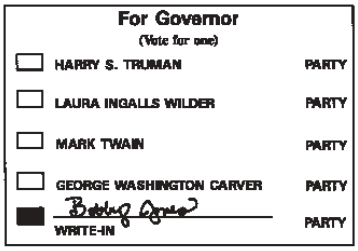
This constitutes an overvote.

(4) In jurisdictions using paper ballots, a valid vote for a write-in candidate must include the following:

(A) A distinguishing mark in the target area next to the name of the candidate;

(B) The name of a qualified write-in candidate. If the name of the candidate, as written by the voter, is substantially as declared by the candidate it shall be counted, or in those circumstances where the names of candidates are similar, the names of candidates as shown on voter registration records shall be counted.

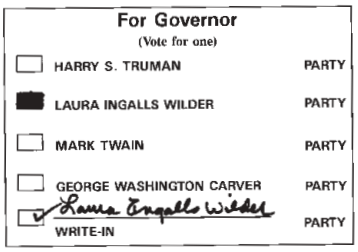
(C) The name of the office for which the candidate is to be elected.



Bobby Jones is a qualified candidate. This constitutes a vote for Bobby Jones.

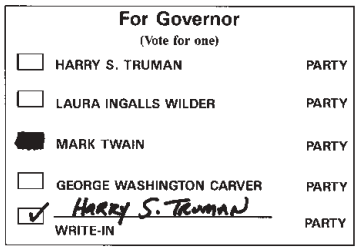
(5) If a voter designates a vote for a named candidate on the ballot and also provides for a write-in candidate in the same race it shall be treated as follows:

(A) If a voter designates a vote for a named candidate on the ballot and writes in the same candidate in the write-in area, the vote shall count for that candidate.



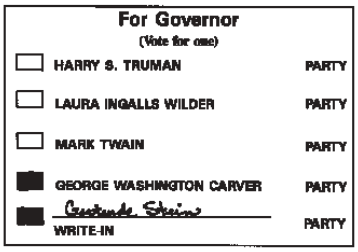
This constitutes a vote for Laura Ingalls Wilder.

(B) If a voter designates a vote for a named candidate on the ballot and writes in the name of a qualified write-in candidate or the name of a different named candidate on the ballot in that race and makes a distinguishing mark in the target area next to the name of the write-in candidate, it shall be considered an overvote with neither candidate receiving credit for the vote.



This constitutes an overvote.

(C) If a voter designates a vote for a named candidate on the ballot and writes in the name of a person who is not a qualified write-in candidate and not a named candidate on the ballot in that race, it shall be considered a vote for the named candidate.



Gertrude Stein is not a qualified candidate. This shall constitute a vote for George Washington Carver.

(6) Whenever a hand recount of votes of paper ballots is ordered, the provisions of this rule shall be used to determine voter intent.

AUTHORITY: section 115.225, RSMo Supp. 2005. Original rule filed Aug. 8, 2001, effective March 1, 2002. Emergency rescis-*

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000517

sion filed Feb. 2, 2006, effective Feb. 18, 2006, expired Aug. 16, 2006. Emergency rule filed Feb. 2, 2006, effective Feb. 18, 2006, terminated April 30, 2006. Emergency rule filed April 20, 2006, effective April 30, 2006, expired Aug. 16, 2006. Rescinded and readopted: Filed Feb. 2, 2006, effective July 30, 2006.

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-9.040 Write-In Stickers

PURPOSE: This rule sets out the procedures for the process of using stickers to vote for write-in candidates.

(1) The sticker shall contain the name of a candidate, office sought, and a distinguishing mark in the square immediately preceding the name of the candidate and shall be approximately one inch by three inches (1" × 3") in size with black print on a white background.

(2) The sticker shall be placed by the voter on the write-in line designating the office sought or the sticker shall be placed by the voter on the write-in line on the secrecy envelope.

AUTHORITY: section 115.439.5, RSMo Supp. 2002. Emergency rule filed Oct. 11, 2002, effective Oct. 21, 2002, expired April 18, 2003. Original rule filed Oct. 18, 2002, effective April 30, 2003.*

**Original authority: 115.439, RSMo 1977, amended 1993, 2002.*

AMERICAN OVERSIGHT

Rules of
Elected Officials
Division 30—Secretary of State
Chapter 10—Voting Machines (Electronic)

Title		Page
15 CSR 30-10.010	Definitions	3
15 CSR 30-10.020	Certification Statements for New or Modified Electronic Voting Systems	4
15 CSR 30-10.025	Election Authority's Certification Statement	5
15 CSR 30-10.030	Voter Education and Voting Device Preparation	5
15 CSR 30-10.040	Electronic Ballot Tabulation—Counting Preparation	8
15 CSR 30-10.050	Election Procedures	9
15 CSR 30-10.060	Electronic Ballot Tabulation—Election Procedures	9
15 CSR 30-10.070	Certificates by Officers; Security Areas; Retention of Material; Independent Audit (Rescinded June 25, 1987)	10
15 CSR 30-10.080	Absentee Balloting	10
15 CSR 30-10.090	Procedure for Recount or Contested Election	13
15 CSR 30-10.100	Rejection of Votes (Rescinded December 13, 1979)	13
15 CSR 30-10.110	Manual Recount	13
15 CSR 30-10.120	Ballot Management Systems	14
15 CSR 30-10.130	Voter Education and Voting Device Preparation (DREs and Precinct Counters)	14
15 CSR 30-10.140	Electronic Ballot Tabulation—Counting Preparation and Logic and Accuracy Testing (DREs and Precinct Counters)	15
15 CSR 30-10.150	Closing Polling Places (DREs and Precinct Counters)	16
15 CSR 30-10.160	Electronic Ballot Tabulation—Election Procedures (DREs and Precinct Counters)	17

AMERICAN OVERSIGHT

Title 15—ELECTED OFFICIALS
Division 30—Secretary of State
Chapter 10—Voting Machines (Electronic)

15 CSR 30-10.010 Definitions

PURPOSE: This rule provides definitions of terms in addition to those found in Chapter 115, RSMo for the conduct of elections.

(1) Election authority shall mean the county clerk or board of election commissioners. The election authority shall be the chief custodian of the electronic voting system and its components and shall be responsible for the proper maintenance and all necessary preparation for elections. The election authority is authorized to appoint as many custodians as deemed necessary and is permitted by law.

(2) Electronic voting system is a system of casting votes by use of marking devices, and counting votes by use of automatic tabulating or electronic data processing equipment and includes computerized voting systems.

(3) Automatic tabulating equipment shall mean a system consisting of a mechanical or photoelectric ballot card reader, or both, an electronic central processing unit and visually readable tabulated results of the voters' markings on the ballot card. Integral to the system is a capacity to determine the number of ballots processed and the votes cast on each candidate and each ballot question by precinct, jurisdiction total and any other needed total such as ward or township. Absentee totals shall be determinable.

(4) Program shall mean the prepared election computer program or the section of the computer program that contains the information for the particular election being tabulated. Additionally the term shall extend to all programs in the system including, but not limited to, system software, utilities software and compilers, which may be used during the operation of the application software which tabulates the ballots. The program may be stored on cards, tapes, discs, integrated circuits or other electronic, magnetic, optical or paper storage media.

(5) Ballot card is a ballot which is voted by making a punch or sensor mark which can be tabulated by automatic tabulating equipment. All types of automatic or electronic system ballots shall be known as ballot cards regardless of size or stock thickness.

(6) Ballot label is the card, paper, booklet, page or other material containing the names of all offices, candidates and questions to be voted on.

(7) Systems which use a single unit for the ballot card and the ballot label shall conform to the rules for both.

(8) Accessible voting station is a voting station equipped for individuals with disabilities.

(9) Audio ballot is a ballot in which a set of offices and issues is presented to the voter in audible, rather than visual form.

(10) Audit trail is recorded information that allows election officials to review the activities that occurred on the voting equipment to verify or reconstruct the steps followed without compromising the ballot or voter secrecy.

(11) Audit trail for direct recording equipment is a paper printout of votes cast, produced by direct recording electronic voting machines (DREs), which election officials may use to crosscheck electronically tabulated totals.

(12) Ballot marking device is any approved device which will enable the votes cast on paper ballots to be counted by automatic tabulating equipment.

(13) Ballot style is the particular set of contests and issues to appear on the ballot for a particular election district, their order, the list of ballot positions for each contest or issue, and the binding of candidate names and issues to ballot positions.

(14) Cast vote record is the permanent record of all votes cast by a single voter whether in electronic, paper or other form.

(15) Counter is the register on each Direct Recording Electronic (DRE) unit which increments by one (1) each time a ballot is cast on the unit. The election counter is the register which is reset for each election and records the number of ballots cast on a DRE unit in a particular election. The system counter is the register which cannot be reset and records the number of ballots cast on a DRE unit over the course of the life of the unit.

(16) DRE is an electronic voting system that utilizes electronic components for the functions of ballot presentation, vote capture, vote recording and tabulation, which are logically and physically integrated into a single unit. A DRE produces a tabulation of the voting data stored in a removable memory component and in printed hard copy.

(17) Election management system is a set of processing functions and databases within a voting system that define, develop and maintain election databases, perform election definition and setup functions, format ballots, count votes, consolidate and report results, and maintain audit trails.

(18) Electronically-assisted ballot marking device is a device that provides assistance to voters who are visually impaired, who have difficulty reading English, or who have difficulty correctly marking by hand a preprinted paper ballot that is to be counted in optical scan systems. The device marks, or assists the voter to mark, selected choices on a previously inserted, preprinted paper ballot. The device then provides audio, tactile, or visual feedback to the voter with regard to the choices the voter has made on the ballot. The completed ballots are later tabulated on the same unit that processes other paper ballots.

(19) Logic and accuracy testing is the testing of the tabulator setups of a new election definition to ensure that the content correctly reflects the election being held (i.e., contests, candidates, number to be elected, ballot styles, etc.) and that all voting positions can be voted for the maximum number of eligible candidates and that results are accurately tabulated and reported.

(20) Paper cast vote record is a paper record of all votes cast by a single voter that can be directly verified by the voter. It is the record that is created from the voter verifiable audit record after the selections are verified and the vote is cast by the voter.

(21) Precinct count voting system is a voting system that tabulates ballots at the polling place. These systems typically tabulate ballots as they are cast and are capable of printing the results after the close of polling.

AUTHORITY: section 115.225, RSMo Supp. 2005. Original rule filed March 31, 1972, effective April 14, 1972. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983. Amended: Filed Dec. 15, 1986, effective Feb. 28, 1987. Emergency amendment filed June 21, 2006, effective July*

AMERICAN OVERSIGHT

1, 2006, expired Feb. 22, 2007. Amended: Filed June 21, 2006, effective Dec. 30, 2006.

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-10.020 Certification Statements for New or Modified Electronic Voting Systems

PURPOSE: This rule provides that voting machine manufacturers file an initial affidavit stating that the voting machine complies with all applicable rules and laws and a second affidavit stating that when any changes are made in the system the voting machine's ability to continue to comply with the applicable rules and laws will not be affected and that voting machine manufacturers deposit into an escrow account the source code for each version of their voting system qualified for sale and use in Missouri.

(1) As a prerequisite to approval from the secretary of state, each manufacturer or supplier of electronic voting systems or equipment shall have completed and submitted to the secretary of state a certification statement in substantially the same form as contained in section (5), and shall have received certification from an independent testing authority approved by the secretary of state.

(2) Beginning on July 1, 2006, when no amendments have been made to an approved system or machine subsequent to qualification, the manufacturer or supplier shall notify the secretary of state that no amendments have been made on a semi-annual basis on January 1 and July 1 starting on the notification date immediately following approval.

(3) As a prerequisite to approval from the secretary of state, each manufacturer or supplier of electronic voting systems or equipment shall execute an escrow agreement with an escrow agent for the manufacturer's source code for each system fully qualified by the Office of the Secretary of State. At a minimum, the agreement must:

(A) Identify an escrow agency;

(B) Provide the software source code for all voting system components in a minimum of two (2) formats (one (1) human readable and one (1) machine readable) to the escrow agent;

(C) Provide the software documentation to the escrow agent;

(D) Contain a statement confirming that the state of Missouri will, within seven (7) days of the occurrence of one of the following events, receive full access to the source code and unlimited rights to continue using and supporting the software at no cost to the state or the agency should the manufacturer:

1. Become insolvent; or

2. Make a general assignment for the benefit of creditors; or

3. File a voluntary petition of bankruptcy; or

4. Suffer or permit the appointment of a receiver for its business or assets; or

5. Become subject to any proceeding of bankruptcy or insolvency law, whether foreign or domestic; or

6. Wind up or liquidate its business voluntarily or otherwise and the state has reason to believe that the vendor will fail to meet future obligations; or

7. Discontinue support of the provided products or fail to support the products in accordance with its maintenance obligations and warranties;

(E) Contain a statement agreeing to notify in writing the Independent Testing Authority (ITA) that certified the system, giving the state of Missouri full access to "final build," records and test results related to the certification tests at no charge to the state; and

(F) Contain a statement agreeing that the escrow will stay in place as long as the system is used in Missouri, at no cost to the state.

(4) If any modification, deletion or improvement to approved voting or tabulating equipment, procedures or systems is made, the manufacturer, programmer or supplier shall notify the secretary of state and a certification amendment statement shall be submitted.

(A) No certification need be submitted if one (1) of the following conditions are met:

1. The equipment is not a device which—

A. Converts the intent of the voter into a data string, as an example, a card reader or scanner;

B. Changes, interprets, converts, modifies or records the data string being transmitted from the ballot counter; or

C. Manipulates data or the results of any data conversion into a report exclusive of the printer; or

2. The software only monitors system operation.

(B) Certificates from the software supplier or programmer shall always be submitted in the following cases when the additions could be used during the tabulating process:

1. Installation of a new release of system software, utilities software, or both;

2. Installation of new or expanded central processing units;

3. Installation of additional random access or read only memory (RAM or ROM); and

4. Installation of additional magnetic, electronic or optical data storage units.

(C) All systems installed as of January 1, 1987 are approved in the configuration that existed as of that date.

(5) Manufacturer's certification statement shall be completed substantially as the example which follows:

MANUFACTURER'S CERTIFICATION STATEMENT

I, _____, president of _____
(*electronic voting systems company*)
do hereby certify to _____, Secretary of State of Missouri that the _____ electronic voting
(name of equipment)
system will permit in accordance with section 115.225, RSMo:

1. Voting in absolute secrecy;

2. Each elector to vote at any election for all persons and offices for whom and for which s/he is lawfully entitled to vote;

3. The automatic tabulating equipment to be set to reject all votes for any office or on any measure except write-in votes when the number of votes exceeds the number the voter is entitled to cast;

4. Each elector to vote for as many persons for an office as s/he is entitled to vote for;

5. Each elector to vote for or against any questions upon which s/he is entitled to vote; and to vote, by means of a single device, where applicable, for all candidates of one (1) party or to vote a split ticket as s/he desires;

6. Each elector, at presidential elections, by one (1) punch or mark, to vote for the candidate of that party for president, vice-president and their presidential electors; and

7. The _____ electronic voting system complies with all other requirements of the election laws of the state of Missouri where they are applicable.

(Briefly describe the type of electronic voting system provided by _____, the means by which it meets the requirements of provisions 1.–6. and list the areas in which the system is in use.)

I do hereby certify that the above information is true and accurate this _____ day of _____ , 20___.

_____
(President)

AMERICAN OVERSIGHT MO-SOS-23-091-PA-000521

_____
(Name of Company)

The above signator appeared before me this _____ day of _____, 20__, and did personally sign this affidavit.

_____
(Notary)

My commission expires _____

(6) Compliance with this certification statement will assist this office when approval is requested for use of electronic voting systems in this state. After receiving this information, the secretary of state will schedule a meeting with the election official making the request to use electronic equipment and representatives of the voting equipment company to discuss approval of its use in Missouri.

(7) The certification amendment statement shall be completed substantially as the example which follows:

AMENDMENT TO CERTIFICATION STATEMENT

I, _____
(Name)
_____, of
(Office)
_____, do hereby certify
(Company)
to _____, Secretary of State of Missouri, that the change outlined here will not affect the accuracy or legal operational requirements as outlined in section 115.225, RSMo of
_____.
(Product Name and Version)

_____
(Briefly describe the change.)

_____
(Signature)

The above signator appeared before me this _____ day of _____, 20___ and did personally sign this affidavit.

_____
(Name)

_____
(Name of Company)

_____
(Notary)

My commission expires _____

(8) No change in system software, utilities software, or both, may be made within six (6) weeks prior to an election in which the automated tabulating equipment will be used for the tabulating of ballots. In the event that system software, utilities software, or both, is to be changed within thirty (30) days after any election in which the automated tabulating equipment is used for the tabulating of ballots, the election authority shall have copies made of the original system software, utilities software, or both, and those copies shall be stored in the same manner as the ballots counted in that election.

AUTHORITY: section 115.225, RSMo Supp. 2005. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed April 7, 1978, effective July 13, 1978. Emergency amendment filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Amended: Filed Oct. 5, 1982, effective Feb. 11, 1983. Amended: Filed Dec. 15, 1986, effective Feb. 28, 1987. Rescinded and readopted: Filed Aug. 8, 2001, effective March 1, 2002. Emergency amendment filed June 21, 2006, effective July 1, 2006, expired Feb. 22, 2007. Amended: Filed June 21, 2006, effective Dec. 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-10.025 Election Authority's Certification Statement

PURPOSE: This rule provides a method by which the election authority and the secretary of state are assured that the systems being purchased are approved for use in Missouri.

(1) No election authority shall authorize payment for software or hardware used for the tabulation of ballots unless the following actions have been taken:

(A) They shall have on file in their office a copy of the letter of authorization from the secretary of state to the manufacturer of the equipment, software, or both, being purchased which states that the equipment, software, or both, is approved for use in Missouri; and

(B) They shall have filed with the elections division of the Secretary of State's office a sworn statement that they do have the letter referenced in section (S) in their file and they believe that the software, equipment, or both, purchased is the same as that approved by the secretary of state.

AUTHORITY: section 115.225, RSMo 1986. Original rule filed Dec. 15, 1986, effective Feb. 28, 1987.*

**Original authority: 115.225, RSMo 1977.*

15 CSR 30-10.030 Voter Education and Voting Device Preparation

PURPOSE: This rule provides for the conduct of voter education and voting device preparation.

PUBLISHER'S NOTE: The secretary of state has determined that the publication of the entire text of the material which is incorporated by reference as a portion of this rule would be unduly cumbersome or expensive. Therefore, the material which is so incorporated is on file with the agency who filed this rule, and with the Office of the Secretary of State. Any interested person may view this material at either agency's headquarters or the same will be made available at the Office of the Secretary of State at a cost not to exceed actual cost of copy reproduction. The entire text of the rule is printed here. This note refers only to the incorporated by reference material.

(1) Before elections in which an electronic voting system is to be used for the first time, the election authority shall conduct a public information program to acquaint voters who will be using the system with the manner in which ballots are voted and counted.

(2) Vote Recording Preparation—Polling Place. In addition to those supplies required for the conduct of elections generally, the election authority shall cause to have prepared and delivered to each polling place using the electronic voting system no later than forty-five (45) minutes prior to the opening of the polls, a sufficient quantity of the following:

(A) Each polling place in a primary or general election shall be provided with at least one (1) voting device for each one hundred fifty (150) registered voters. A sufficient number of machines shall be provided for other elections. There shall always be one (1) extra specimen voting device per polling place for use in the instruction of voters. Exceptions to this regulation for specific elections may be granted upon application therefor to the secretary of state. In primary elections there shall be at least one (1) voting device for each eligible political party or ticket. The voting devices shall be put in order, set, adjusted and ready for voting when delivered to the polling places;

(B) Ballot label assemblies for use on voting devices requiring ballot labels, in the format approved by the secretary of state, properly sequenced, mounted in each voting device supplied. The type of election and the date of election shall be plainly marked on

AMERICAN OVERSIGHT

the front cover of each ballot label assembly. In preparing a voting device for an election, it shall be arranged so that it will in every particular case meet the requirements for voting and counting at that election;

(C) Ballot cards in the form required for processing by the electronic data processing equipment. The number of ballot cards supplied shall be sufficient to comply with section 115.247, RSMo;

1. The ballot card shall be in the format approved by the secretary of state. In the case of ballot cards of the 5081 size, the ballot stub and the ballot card shall not contain any common identifying mark, number or symbol which would permit them to be matched after having been detached in the voting process. Systems using larger sheets for ballot cards shall likewise be void of matching marks.

2. All arrows on the ballot label indicating where a voter may mark to designate his/her vote shall point to the center of the appropriate hole in the mask or the proper area for marking. All play in the ballot label of the 5081 size cards shall be limited so that the point of the arrow always points to the hole.

3. Demonstration ballot cards of a distinctive color, clearly marked for demonstration for use in the instruction voting device to educate the voter in the use of the system shall be supplied in such number as may be determined by the election authority.

4. Sample ballots, demonstration ballot cards or ballot labels which shall be exact copies of the official ballots except for wording indicating the sample status of the sheet.

5. All ballot cards shall be delivered to the polling places in a sealed package or container;

(D) Envelopes, sufficient in size to cover the voting area of the ballot card, if ballot cards of the 5081 format are used, made of stiff paper into which the ballot card is inserted by the voter after voting. The envelope shall cover the voting area of the ballot card and shall be of sufficient width to prevent insertion into a voting device. Ballot envelopes shall contain space so that the voter may cast write-in votes, if allowable for that election. The number of ballot envelopes shall equal the number of ballot cards supplied. Envelopes shall not be required in systems where the voter inserts the ballot card into the electronic counting device him/herself;

(E) Paper ballots, if any part of the election is to be voted on paper ballots;

(F) Ballot boxes as required by general election law;

(G) A transfer case sufficiently large to hold, transfer to the counting location from the polling place and store the ballot cards which have been voted in a polling place and the spoiled ballots envelope. The transfer case shall be constructed of metal and sealed with a numbered nonreusable seal;

(H) Envelopes and containers in which to enclose voted paper ballots, if used; spoiled ballot cards; envelopes; unused paper ballots; and unused ballot cards;

(I) A ballot card certificate, in the form set out with this rule, together with an envelope addressed to the election authority;

(J) Two (2) sample ballots of each ballot type to be voted on in the polling place;

(K) Pencils, seals and any other supplies and forms deemed necessary; and

(L) *Instruction Guide for Election Judges and Clerks* issued by the secretary of state.

AUTHORITY: section 115.225, RSMo 1986. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed Sept. 15, 1972, effective Sept. 25, 1972. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983.*

**Original authority: 115.225, RSMo 1977.*

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000523

STATE OF MISSOURI
BALLOT CARD CERTIFICATION

This section to be completed BEFORE Polls open.

We hereby certify at the _____Election held in _____, Missouri, on _____, 19 _____ in _____ Township and _____Precinct(s) that the following information is correct.

_____ _____
(Initials of Judges)

Rep. _____ Dem. _____
Rep. _____ Dem. _____
Rep. _____ Dem. _____

BALLOT SERIAL NUMBERS

_____ _____

Color _____ Beginning No. _____ Ending No. _____ Total _____
Color _____ Beginning No. _____ Ending No. _____ Total _____

Total Ballots Received _____

This section to be completed AFTER Polls close.

Total number of spoiled ballots _____
Total number of unused ballots (all colors) _____
Total number of ballots removed from ballot box after polls close _____

Total of 3 lines above _____

Total number of signed ID cards (must equal total ballots from box) _____
Total number of envelopes containing write-in votes _____

SIGNATURES OF ELECTION JUDGES

Rep. _____ Dem. _____
Rep. _____ Dem. _____
Rep. _____ Dem. _____

Transfer Case Seal Number _____

Transfer Case has been received at the counting location and the contents have been checked in.

_____ _____ _____
(Dem.) *(Rep.)* *(Time)*

AMERICAN OVERSIGHT

15 CSR 30-10.040 Electronic Ballot Tabulation—Counting Preparation

PURPOSE: This rule provides for procedures in connection with the preparation for vote recording and tabulation including appointment of judges, equipment and program preparation and pre-election testing.

(1) The election authority shall be responsible for insuring that the electronic tabulating system s/he chooses to use accurately records, and/or counts, all proper votes cast and complies with all applicable state statutes and rules.

(2) The election authority shall be responsible that all steps have been taken to insure that the electronic tabulating equipment operates properly at the time of the pre-election public logic and accuracy test and during the tabulation of ballots on election night.

(3) The election authority shall be responsible for making necessary arrangements for a backup ballot tabulating system.

(4) The election authority shall be responsible for providing a duplicate of the counting program for the computer system on which the ballot tabulation is to be done, regardless of the backup counting system used.

(5) Prior to each election day, the election authority shall be responsible for appointing one (1) or more bipartisan teams composed of equal numbers of members from the two (2) major parties to carry out the functions of—certifying the accuracy of the electronic tabulating equipment, receiving election materials from the polls, duplicating damaged or defective ballots, processing ballots through the electronic tabulating system and preparing election materials for final storage. Each person so appointed shall have the qualifications of and take the oath of office prescribed for election judges in section 115.091, RSMo. These persons will be selected from lists compiled as outlined in section (6) except where an election authority is a board of election commissioners, the election authority may designate persons of its own choosing.

(6) Beginning in 1987, not less than sixty (60) days prior to the first election date of each calendar year, each election authority, except as noted in section (5), shall notify by mail, the chairpersons of the two (2) major political parties within their jurisdiction of the number of persons from their parties needed for the bipartisan teams used in processing and counting ballots. Each chairperson shall have thirty (30) days to provide a list to the election authority, in writing, of twice as many persons meeting the qualifications of section 115.091, RSMo, as the election authority has indicated are necessary. If the chairpersons cannot respond in that thirty (30)-day period with the list of names or enough persons to fill all positions, the election authority shall select persons from that party to fulfill those functions. Nothing contained in this rule shall prohibit an election authority from requesting a new list of names for the bipartisan teams for each election provided that the lists are requested sixty (60) days prior to the election and that the chairpersons have thirty (30) days for response. For elections in 1986, the election authority shall select members of the bipartisan teams in a manner consistent with the way in which s/he has previously selected these personnel. If the election authority has not previously utilized automated tabulating equipment, it shall follow the same schedule as will be used in succeeding years except that the chairpersons shall be notified not later than sixty (60) days prior to the August primary.

(7) Prior to election day the election authority shall supervise a public logic and accuracy test of the electronic tabulating equipment conducted by the accuracy certification team.

(A) The logic and accuracy test shall be open to any member of the public; and the election authority, by some appropriate method, shall notify the public of the time and date of the test.

(B) Persons, other than candidates and other individuals required to be notified under section 115.233, RSMo, wishing to participate in the testing process shall file a written request with the election authority at least twenty-four (24) hours prior to the publicized beginning of the logic and accuracy test.

(C) The election authority shall prepare an appropriate logic and accuracy test deck which will include the following conditions:

1. Each ballot position must be tested;

2. No two (2) candidates for the same office may receive the same number of votes, but each candidate must receive one (1) vote;

3. No ballot question may receive the same number of votes for and against;

4. In situations where a voter can legally vote for more than one (1) person for an office, at least one (1) card shall be voted for the maximum number of allowable candidates;

5. One (1) card shall be marked to have one (1) more vote for each candidate or question than is allowable;

6. One (1) card shall have no votes recorded on it;

7. In general partisan elections, each party shall receive at least one (1) straight party vote. Additionally each party shall receive at least one (1) straight party vote where a candidate of another party receives a vote on the ballot;

8. Ballots should be punched or marked to test all name rotations, if used; and

9. One (1) card (if possible) shall contain a vote for a candidate for whom persons using that ballot format are not entitled to vote.

(D) The accuracy certification team may run the test deck as provided by the election authority again, making as many additions, subtractions or changes in the ballot cards as they desire.

(E) The public logic and accuracy team shall compare the results of the electronic test to those from a manual count of the test ballots. If the results are incorrect, then changes and/or corrections will be made until an errorless count is made. An electronic ballot tabulation machine shall not be used on election day until an errorless count is made on that machine.

(F) After the team is satisfied that the equipment is tabulating the ballots properly, each candidate on the ballot or any representative of a group which has notified the election authority pursuant to subsection (7)(B) may inspect and manually recount the test deck.

(G) If the results match with the manual count, the team shall certify that the system is accurate and properly counting ballots. All logic and accuracy test materials including the deck shall be sealed in a tamperproof container and sealed with a numbered seal. All team members shall verify, by signature or initials, the seal number on a certificate placed on the outside of the container.

(H) The election authority shall have custody of the logic and accuracy test materials including the program until called for by the accuracy certification team.

AUTHORITY: section 115.225, RSMo 2000. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed April 7, 1978, effective July 13, 1978. Emergency rescission and rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983. Emergency rescission and rule filed May 12, 1986, effective Aug. 1, 1986, expired Nov. 7, 1986. Emergency rescission and rule filed April 17, 1987, effective April 27, 1987, expired Aug. 14, 1987. Rescinded and readopted: Filed April*

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000525

17, 1987, effective June 25, 1987. Rescinded and readopted: Filed Aug. 8, 2001, effective March 1, 2002.

**Original authority: 115.225, RSMo 1977, amended 1993, 1995.*

15 CSR 30-10.050 Election Procedures

PURPOSE: This rule provides for the appointment and instruction of election judges.

PUBLISHER'S NOTE: The secretary of state has determined that the publication of the entire text of the material which is incorporated by reference as a portion of this rule would be unduly cumbersome or expensive. Therefore, the material which is so incorporated is on file with the agency who filed this rule, and with the Office of the Secretary of State. Any interested person may view this material at either agency's headquarters or the same will be made available at the Office of the Secretary of State at a cost not to exceed actual cost of copy reproduction. The entire text of the rule is printed here. This note refers only to the incorporated by reference material.

(1) The election authority shall appoint a minimum of four (4) judges for each polling place to be used in the election according to sections 115.079, 115.081 and 115.083, RSMo.

(2) All persons not previously trained in the use of the type of voting equipment being used, prior to entering into the performance of their duties as judges at the election, shall attend a course of instruction for judges in the use and operation of the electronic voting system, conducted under the authorization and supervision of the election authority. In addition to the normal duties of the judges of election, the instruction shall cover the proper use and procedures for use of the voting devices, ballot cards, marking of the ballot cards, procedures for write-in votes (when applicable), replacing spoiled ballots and procedures for safeguarding and transfer of ballot cards and other materials.

(3) The voting and marking devices, registration books, identification cards, ballots and other necessary supplies shall be delivered to the polling places prior to 5:30 a.m. on election day.

(4) Instructions to Election Judges. The election authority shall provide the *Instruction Guide for Election Judges* issued by the secretary of state to be given to election judges in each polling place. All election procedures outlined in the instruction guide will be performed by judges in polling places having electronic voting systems.

AUTHORITY: section 115.225, RSMo 1986. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed Sept. 15, 1972, effective Sept. 25, 1972. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983.*

**Original authority: 115.225, RSMo 1977.*

15 CSR 30-10.060 Electronic Ballot Tabulation—Election Procedures

PURPOSE: This rule provides for procedures to be used by election authorities using electronic tabulating equipment to count voted ballots.

(1) Voted and unvoted ballots shall be processed using the following rules:

(A) Voted ballots shall always be handled or moved either by a bipartisan team or in the direct view of a bipartisan team;

(B) In those cases where the election authority determines it is more efficient to move voted ballots by use of a single person, those items shall be placed into a tamperproof container and sealed with a numbered seal. Members of a bipartisan team shall witness the sealing and verify the number of the seal by their signatures on a certificate placed on the exterior of the container. The container shall only be opened in the presence of a bipartisan team which shall verify the accuracy of the seal number before the seal is broken;

(C) The election authority shall be responsible for insuring that sufficient certificates are made on each transfer of ballot responsibility to accurately recreate each movement of the ballot from one (1) team to the next. Each transfer shall include a statement that no election material was added, subtracted or altered except as provided by statute or rule and that no irregularities were noticed unless otherwise noted; and

(D) The election authority or his/her representative shall be on hand at all times in the counting center when ballots are unsealed.

(2) Ballot counting shall be conducted as follows:

(A) The election authority shall have the authority to limit access by persons, other than those previously appointed to bipartisan teams, in those areas where ballots are unsealed or are being counted;

(B) Ballot duplication for damaged ballots shall be done by bipartisan teams using whatever method is selected by the election authority provided that—

1. The system provides an exact duplicate of the voter's intent, pursuant to 15 CSR 30-9.010, 15 CSR 30-9.020 and 15 CSR 30-9.030;

2. Both members of the team participate in the process;

3. Both members can review the other's work;

4. There is an undisputed method to match the duplicate card with its original after it has been placed with the remainder of the ballot cards from that precinct; and

5. Allowances are made for watchers appointed pursuant to section 115.107, RSMo to perform their statutory duties;

(C) Any changes to the operating system, application programs, files or counters used in the ballot counting shall be documented by the election authority;

(D) The last transaction with the electronic tabulating system prior to counting ballots shall be the public logic and accuracy test; and

(E) The election authority may conduct other logic and accuracy tests as s/he deems necessary including the hand count of ballots.

(3) Prior to certification of the election results, the accuracy and certification team shall recount the test deck used prior to the start of ballot tabulation on each electronic tabulating machine as follows:

(A) In the event that the counts are not identical, the team shall not certify that the electronic tabulating system was operating properly;

(B) Necessary corrections shall be made to the tabulating program until the test deck is counted properly, and all ballots shall be recounted; and

(C) If the counts are identical, the team shall certify that the system is operating properly.

(4) After the accuracy certification team has approved the count and before the ballots are sealed for final storage, the team processing the ballots shall select one (1) precinct by mutual consent to be recounted. The results of that recount shall be reported on certificates supplied by the secretary of state. One (1) copy shall be filed with the secretary of state within four (4) weeks of the election date and one (1) copy shall be filed with the public records of the election.

AMERICAN OVERSIGHT

(5) After the recount of the selected precinct, bipartisan teams shall place all ballots and other support materials into appropriate tamperproof containers which are sealed in such a way as to prevent any undisclosed entry. If numbered seals are used, those numbers shall appear on the exterior of the container and shall be witnessed by the signatures of the team members.

AUTHORITY: section 115.225, RSMo 2000. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed Sept. 15, 1972, effective Sept. 25, 1972. Amended: Filed Nov. 18, 1976, effective March 11, 1977. Emergency amendment filed Oct. 8, 1976, effective Oct. 18, 1976, expired Feb. 15, 1977. Amended: Filed April 7, 1978, effective July 13, 1978. Emergency rescission and rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983. Emergency rescission and rule filed May 12, 1986, effective Aug. 1, 1986, expired Nov. 7, 1986. Emergency rescission and rule filed April 17, 1987, effective April 27, 1987, expired Aug. 14, 1987. Rescinded and readopted: Filed April 17, 1987, effective June 25, 1987. Rescinded and readopted: Filed Aug. 8, 2001, effective March 1, 2002.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995.*

15 CSR 30-10.070 Certificates by Officers; Security Areas; Retention of Material; Independent Audit
(Rescinded June 25, 1987)

AUTHORITY: section 115.225, RSMo 1986. Original rule filed March 31, 1972, effective April 10, 1972. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983. Emergency rescission filed April 17, 1987, effective April 27, 1987, expired Aug. 14, 1987. Rescinded: Filed April 17, 1987, effective June 25, 1987.

15 CSR 30-10.080 Absentee Balloting

PURPOSE: This rule sets out procedures for absentee balloting in addition to those found in Chapter 115, RSMo.

PUBLISHER'S NOTE: The secretary of state has determined that the publication of the entire text of the material which is incorporated by reference as a portion of this rule would be unduly cumbersome or expensive. Therefore, the material which is so incorporated is on file with the agency who filed this rule, and with the Office of the Secretary of State. Any interested person may view this material at either agency's headquarters or the same will be made available at the Office of the Secretary of State at a cost not to exceed actual cost of copy reproduction. The entire text of the rule is printed here. This note refers only to the incorporated by reference material.

(1) All jurisdictions using electronic data processing tabulation systems may conduct absentee balloting by the same means. The requirements of Chapter 115, RSMo shall be followed.

(2) For absentee ballots to be voted within the office of the election authority, the election authority may provide voting devices equipped with ballot label assemblies as provided in 15 CSR 30-10.030 or by voting on the styrofoam-type backing in the case of the 5081 type ballot cards in the same manner as does the voter who receives an absentee ballot by mail.

(3) For absentee ballots to be voted elsewhere, the election authority shall provide:

(A) A ballot card mounted on a backing of styrofoam or other similar material to permit convenient and efficient marking of the ballot card if the 5081 type card is used. Ballot cards where the mark is by way of a pencil do not require the backing materials;

(B) A disposable marking device for marking the ballot card;

(C) A printed paper listing of the offices, candidates and questions containing reproductions of the pages of the ballot label assembly used for voting;

(D) Absentee voting instructions in substantially the same form as section (6) of this rule;

(E) Ballot card envelope, if used; and

(F) Envelope for returning voted ballot to election authority.

(4) The absentee ballots so voted shall be counted in the manner provided in section 115.301, RSMo.

(5) The absentee ballots should then be processed in accordance with the "Procedures After the Polls Close" outlined in the *Instruction Guide for Election Judges and Clerks*.

(6) Absentee voting instructions are shown in Exhibits 3A and B.

AUTHORITY: section 115.225, RSMo 1986. Original rule filed March 31, 1972, effective April 10, 1972. Amended: Filed Sept. 15, 1972, effective Sept. 25, 1972. Emergency amendment filed Oct. 8, 1976, effective Oct. 18, 1976, expired Feb. 15, 1977. Amended: Filed Nov. 18, 1976, effective March 11, 1977. Amended: Filed April 7, 1978, effective July 13, 1978. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983.*

**Original authority: 115.225, RSMo 1977.*

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000527

EXHIBIT 3A
Sample Absentee Voting Instructions
For Punch Card Voting Jurisdictions

ABSENTEE VOTING INSTRUCTIONS

READ ALL INSTRUCTIONS BEFORE VOTING

Your 'ballot packet' consists of:

- BALLOT CARD (which is mounted on styrofoam backing)
- Ballot Card Secrecy envelope (gray)
- Absentee ballot envelope in which Ballot Card and Secrecy envelope will be inserted
- Official Absentee ballot sheet listing offices, candidates and/or questions
- Absentee Voting Instructions (this sheet)
- Wire Punch device (paper clip)

If you spoil your ballot card in any manner—you may return the ballot packet to the Election Authority and request a new ballot card.

TO VOTE

Read the Official Absentee Ballot sheet noting the offices, the candidate names, questions and other special instructions. Next to the name of each candidate and question is a NUMBER or set of numbers which correspond to numbers on the ballot card.

Using the wire punch device supplied, firmly punch out the small "black dot" on the ballot card above the number of the candidate or issue.

Punch with sufficient force so that the "black dot" is completely punched out of the ballot card.

AFTER VOTING THE BALLOT CARD

- Place the ballot card in the gray secrecy envelope.
- In the presence of a notary public fill out the envelope including your signature. Let the notary sign, date and emboss the envelope.
- Place the ballot card (inside the secrecy envelope) inside the large envelope after the notary fills out his section and completes the embossing.
- Seal the large envelope.
- Return the envelope to the Election Authority either in person or by the U.S. Postal Service.

The envelope containing your ballot must be received by the Election Authority not later than 7 p.m. on the day of the election.

AMERICAN OVERSIGHT

EXHIBIT 3B
Sample Absentee Voting Instructions
for Mark Sense Voting Jurisdictions

ABSENTEE VOTING INSTRUCTIONS

INSTRUCTIONS FOR MARKING BALLOT(S)

USE ONLY THE PENCIL PROVIDED VOTE BOTH SIDES OF BALLOT

1. On receipt of this ballot the voter, using the pencil provided, shall prepare the ballot for voting in the following manner.

(1) Should the voter desire to vote a "straight party ticket" he shall place a cross (X) mark in the circle immediately below the party name. If the voter desires to vote for one or more candidates on more than one party ticket, by voting what is commonly known as a "split ticket" he may place a cross (X) mark in the circle immediately below one party name and mark cross (X) marks in the squares at the left of the names of candidates on other tickets for whom he wishes to vote.

(2) If the voter desires to vote for one or more candidates whose name or names do not appear on the printed ballot, he may do so by writing the name of the person for whom he desires to vote, and placing a cross (X) mark in the square at the left of such name on the printed ballot in the column provided for write-ins.

(3) Where there are two or more candidates for like office in a group, a cross (X) mark in the square to the left of a candidate's name automatically votes against the candidate whose name appears within the same horizontal lines in the column under the circle in which appears the cross (X) mark.

2. All candidates of the party whose circle is marked shall be counted as voted for, excepting where squares are crossed preceding the names of the candidates in other columns. If two or more candidates for the same office are thus designated, neither shall be counted. If the cross (X) is not placed in the circle immediately below the party name at the head of the column, but does appear in the squares opposite the various candidates' names, then only these names shall be counted for, and none other. A cross (X) mark is any line crossing any other line at any angle within the voting space and no ballot shall be declared void because a cross (X) mark therein is irregular in form.

3. It is unlawful to deface or tear a ballot in any manner or to erase any printed name, figure, word or letter therefrom, or to erase any mark made thereon by the voter.

4. A ballot without any marks shall not be counted. Ballots shall be counted only for the person for whom the marks thereon are applicable; when a voter places a mark against two or more names for the same office, and only one candidate is to be chosen for the office, none of the candidates is deemed to have been voted for and the ballot shall not be counted for either candidate.

5. DO NOT FOLD BALLOT. All ballots must be returned to the election authority no later than 7:00 p.m. on election day in order to be counted.

AMERICAN OVERSIGHT

MO-SOS-23-0911-A-000529

15 CSR 30-10.090 Procedure for Recount or Contested Election

PURPOSE: This rule provides program tabulating and accuracy tests in addition to those set out in 15 CSR 30-10.020 for tabulating a recount or contested election.

(1) Procedure for Recall Contest Using Electronic Data Processing System. A recall contest has two (2) parts. Part 1 consists of a yes or no vote for the recall proposal. Part 2 consists of candidates for the vacant office in the event a majority of yes votes are cast for the recall proposal. Only voters casting valid votes in Part 1 are eligible to vote in Part 2. Ballot cards which do not contain a vote in Part 1 and ballot cards which contain both yes and no votes in Part 1 represent invalid ballots not eligible to vote in Part 2, and must be manually removed from the ballot cards to be tabulated with the electronic processing system. Once the invalid ballot cards have been identified manually and have been put aside, and the total removed has been verified, the remaining valid ballot cards are processed to determine the number of yes and no votes for the recall proposal and the candidate(s) elected to succeed the incumbent.

(2) Standard electronic data processing tests and auditing procedures shall be used to test the accuracy and validity of the programming of the electronic data processing system.

AUTHORITY: section 115.225, RSMo 1986. Original rule filed March 31, 1972, effective April 15, 1972. Emergency rescission filed Oct. 5, 1982, effective Nov. 2, 1982. Emergency rule filed Oct. 5, 1982, effective Nov. 2, 1982, expired Feb. 2, 1983. Rescinded and readopted: Filed Oct. 5, 1982, effective Feb. 11, 1983.*

**Original authority: 115.225, RSMo 1977.*

15 CSR 30-10.100 Rejection of Votes
(Rescinded December 13, 1979)

AUTHORITY: section 115.225, RSMo 1978. Original rule filed Nov. 13, 1978, effective Feb. 11, 1979. Rescinded: Filed Aug. 14, 1979, effective Dec. 13, 1979.

15 CSR 30-10.110 Manual Recount

PURPOSE: This rule provides a method for the election authority, the secretary of state and the general public to compare electronically tabulated vote results with manual recounts of selected races and ballot issues in certain election precincts.

(1) Definitions.

(A) County—whenever the word county is used in this rule, it includes the cities of St. Louis and Kansas City.

(B) Precinct—the election authority, at his/her discretion, may consider polling sites containing more than one (1) precinct to be counted as a single precinct for all purposes of this rule.

(2) Prior to the certification of the election results, the accuracy certification team shall randomly select not less than five percent (5%) of all election precincts through the use of a random drawing, but not less than one (1) precinct, in order to conduct a manual recount of selected contested races and ballot issues in the selected precinct(s). Random selection of the precincts shall be open to any member of the public, and the election authority shall notify the public of the time and place of the selection process no later than forty-eight (48) hours prior to the beginning of the selection process by posting a notice in a prominent place, which is easily accessible to the public and clearly designated for that purpose, at the principal office of the election authority.

(3) Recount of the randomly selected precinct(s) shall be conducted in the following manner:

(A) The election authority shall select not less than one (1) manual recount team made up of not less than two (2) persons selected from lists as outlined in 15 CSR 30-10.040(6) except when an election authority is a board of election commissioners, the election authority may designate persons of its own choosing. Each person so appointed shall have the qualifications of and take the oath of office prescribed for election judges in section 115.091, RSMo. The election authority may utilize the accuracy certification team selected in 15 CSR 30-10.040;

(B) For the selected precinct(s), the manual recount team shall unseal the appropriate ballot containers and manually recount certain randomly selected contested races and ballot issues; and

(C) One (1) contested race or ballot issue to be manually recounted shall be randomly selected from each of the following categories, where applicable:

1. Presidential and Vice-Presidential electors, United States senate candidates and state-wide candidates;
2. State-wide ballot issues;
3. United States representative candidates and state general assembly candidates;
4. Partisan circuit and associate circuit judge candidates and all nonpartisan judicial retention candidates;
5. In addition to the candidates and issues previously listed, the manual recount team shall select not less than one (1) contested race or ballot issue from all political subdivisions and special districts, including the county, in the selected precinct(s); and
6. In addition to the candidates and issues previously listed, the manual recount team shall select all races in which the margin of victory between the two (2) top candidates is equal to or less than one-half of one percent (0.5%) of the number of votes cast for the office or issue.

(4) If the results of the manual recount of the selected races and ballot issues differ by more than one-half of one percent (0.5%) from the results of the electronically tabulated vote results, the manual recount team shall immediately notify the election authority, who shall investigate the causes of any discrepancy and resolve any discrepancies prior to the date of certification set forth in section 115.507, RSMo.

(5) The secretary of state, at his/her sole discretion, and upon the showing of good cause by an election authority not less than three (3) weeks prior to the date of an election, may waive the manual recount requirement for any political subdivision or special district holding an election on the election date.

(6) Upon completion of the manual recount, the manual recount team shall reseal the ballots and other support materials in the appropriate containers. The results of the manual recount shall be reported on certificates provided by the secretary of state. One (1) copy shall be filed with the secretary of state within four (4) weeks of the election date and one (1) copy shall be filed with the public records of the election.

(7) The secretary of state may make grant funds available to reimburse election authorities for the cost of conducting manual recounts under section (2) and paragraph (3)(C)6. of this rule.

AUTHORITY: section 115.225.1., RSMo Supp. 2008. Original rule filed Jan. 3, 1990, effective March 26, 1990. Emergency amendment filed Sept. 15, 2008, effective Sept. 25, 2008, expired March 23, 2009. Amended: Filed Sept. 15, 2008, effective March 30, 2009.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002, 2006.*

AMERICAN OVERSIGHT

15 CSR 30-10.120 Ballot Management Systems

PURPOSE: This rule provides that management controls shall be instituted by local election authorities on ballot cards counted by electronic ballot tabulating equipment.

(1) Definitions.

(A) Ballot cards—the computer card on which a voter indicates their votes in the case of a punch card system or the entire ballot on which a voter marks their votes in the case of an optical scan system.

(B) Destruction of ballot cards—any method which renders the cards unusable for further use as ballot cards including burning, mechanical shredding or cutting and chemical decomposition but does not include landfilling or burying.

(2) All county election officials shall develop and operate a management system to document on the public record the acquisition and usage of all ballot cards provided to them for use in automated tabulating systems.

(3) At a minimum, the system shall provide an ongoing inventory record and a signed written affidavit on the public record for the following activities:

(A) Receipt of ballot cards including date of receipt, total shipment received and serial numbers (if available) of the ballot cards;

(B) Issuance of ballot cards to each polling place including the election date, total number of ballot cards issued and serial numbers, if available;

(C) Receipt of ballot cards from each polling place following the election including election date, a reconciliation for each precinct showing total ballots issued, total ballots voted, total ballots invalidated, total ballots lost and total ballots returned unvoted. The election authority within thirty (30) days after the election shall verify by physical count the number of unvoted ballots. Unvoted ballots shall be shown by serial numbers, if available;

(D) Issuance of ballots to the election authority for the purpose of absentee ballot preparation. This record shall contain all the elements contained in subsection (3)(B). Following the election, the election authority shall complete a record containing all information contained in subsection (3)(C);

(E) Destruction of unvoted ballots for whatever purpose the election authority deems appropriate. This record shall contain the number of ballots destroyed, the method of destruction and the serial numbers of the ballot cards, if available;

(F) Issuance of ballots for educational, testing or any purposes other than those mentioned in subsections (3)(A)–(E). In every case the record shall indicate the purpose for which the ballot cards are issued, the serial numbers of the ballots, if available, and the steps taken by the election authority, including the marking of the word VOID on the face or back of the ballot card or changes to the ballot card to insure that the ballot cards will not be used in subsequent elections; and

(G) All the affidavits in this section shall be maintained in the office of the election authority for a period of two (2) years after the date on which all ballot cards from a single shipment of ballot cards have been completely issued.

(4) Each election authority shall conduct an annual inventory of all ballot cards in their custody comparing the actual number of ballot cards in their custody with the number of cards indicated as being on their inventory records.

(A) This inventory must include verification of all serial numbers if available.

(B) The election authority shall establish the date(s) of the inventory at their discretion between April 1 and June 1 of each year.

(C) Following the required inventory, the election authority shall sign an affidavit including the actual number of ballots on hand at the end of the previous inventory, the number of ballots received since the previous inventory, the number of ballots restocked following elections or other activities outlined in section (3), the number of ballots issued or destroyed since the last inventory based on previously filed affidavits, the actual number of ballots on hand as determined by the present inventory and any discrepancies. In the case of discrepancies, the election authority shall include their assessment of the reason for the discrepancy. In all cases the affidavit shall include serial numbers, if available.

(D) One (1) copy of the affidavit shall be held by the election authority in their office for five (5) years from the date of affidavit and one (1) copy shall be forwarded to the secretary of state.

AUTHORITY: section 115.225.1., RSMo 1986. Original rule filed Jan. 3, 1990, effective March 26, 1990.*

**Original authority: 115.225, RSMo 1977.*

15 CSR 30-10.130 Voter Education and Voting Device Preparation (DREs and Precinct Counters)

PURPOSE: This rule provides for the conduct of voter education and preparation of Direct Recording Electronic voting systems (DREs) and Optical Scan Precinct Count voting systems (Precinct Counters).

(1) Before elections in which a direct recording electronic (DRE) or Precinct Counter is to be used for the first time, the election authority shall conduct a public information program to acquaint voters who will be using the system with the manner in which ballots are voted and counted.

(2) DREs and Precinct Counters shall be tested in accordance with section 115.233, RSMo and 15 CSR 30-10.140, using test scripts and testing procedures appropriate for the make, model, and version of the system.

(3) Each memory component must be programmed in a secured facility under the supervision of the election authority or their designated representative. Before and after programming, all memory cards shall be kept in a secure area until inserted into an assigned unit prior to the election and the local election authority must maintain a written log that records all access and transfers of all memory components.

(4) In addition to the standard displayed ballot, the election authority shall ensure that alternative format ballots are available, including, but not limited to a ballot with large print and an audio ballot for use with DREs and with electronically-assisted ballot marking devices.

(A) The election authority shall ensure that any alternative format ballot conforms to federal voting equipment guidelines, provides the same information presented to voters in the standard displayed ballot and can be cast and counted as a secret ballot.

(B) The election authority shall ensure that the order and content of any large print ballot are presented in a manner that is consistent with that of the standard ballot.

(C) The election authority shall ensure that the audio ballot is recorded correctly and that the names of the candidates are pronounced correctly in the audio recordings. The election authority shall also ensure that no candidate's name; political party, political body, or independent designation; incumbency; or other such information nor any ballot issue or answer or response thereto is emphasized, stressed or otherwise inflected in any manner to distinguish a particular candidate, party or body, issue, answer or response to a ballot issue either negatively or positively or to suggest whether to vote for or against such candidates or issues in such audio recordings.

AMERICAN OVERSIGHT MO-SOS-23-0911-A-000531

(5) Vote Recording Preparation—Polling Place. In addition to those supplies required for the conduct of elections generally, the election authority shall cause to have prepared and delivered to each polling place using DREs and Precinct Counters no later than forty-five (45) minutes prior to the opening of the polls, a sufficient quantity of the following:

(A) In jurisdictions in which DREs are the principal system used to cast votes, each polling place in a primary or general election shall be provided with at least one (1) DRE for each one hundred fifty (150) registered voters. A sufficient number of DREs shall be provided for other elections. A sufficient number of assistive devices (i.e., sip-and-puff input devices, headphones, etc.) shall be provided for use with each unit provided. The DREs shall have been put in order, set, adjusted, and ready to open for voting when delivered to the polling places;

(B) In jurisdictions in which DREs or electronically-assisted ballot marking devices are used to provide an accessible voting station, at least one (1) DRE or one (1) ballot marking device shall be provided in each polling location with a sufficient number of assistive devices (i.e., sip-and-puff input devices, headphones, etc.) for use with each unit provided. The units shall have been put in order, set, adjusted, and ready to open for voting when delivered to the polling places;

(C) In jurisdictions in which Precinct Counters are the principal system used to cast votes, each polling place shall be provided with at least one (1) Precinct Counter. The Precinct Counter(s) shall have been put in order, set, adjusted, and ready to open for voting when delivered to the polling places;

(D) Voter access or activation cards or devices programmed with the correct ballot styles for each polling location, in quantities sufficient to conduct the election and delivered to the polling place in a secure container securely sealed in such a manner that if the container is opened, the seal will be broken beyond repair;

(E) Ballot boxes as required by general election law;

(F) Optical Scan paper ballots in locations using Precinct Counters, provisional ballots, provisional ballot envelopes and spoiled ballot envelopes in all locations;

(G) Pencils, seals, rolls of paper for DRE paper cast vote record printers and other supplies and forms deemed necessary;

(H) *Instruction Guide(s) for Election Judges and Clerks,* for the system(s) being used, issued by the secretary of state. In addition to the Instruction Guide issued by the secretary of state, the local election authority may include instructional materials developed by the local election authority for each system used at that polling location;

(I) A transfer case sufficiently large to hold, transfer to the central location from the polling place and store paper cast vote records, electronic media, any paper ballots which have been voted in a polling place and any spoiled ballot envelopes. The transfer case shall be constructed of durable material and tamperproof design and securely sealed in such a manner that if the case is opened, the seal will be broken beyond repair;

(J) Two (2) sample ballots of each ballot to be voted on in the polling place; and

(K) Privacy sleeves for ballots or paper cast vote records that are carried by the voter from one location in the polling place to another for verification purposes and that are not otherwise covered.

AUTHORITY: section 115.225, RSMo Supp. 2005. Emergency rule filed June 21, 2006, effective July 1, 2006, expired Feb. 22, 2007. Original rule filed June 21, 2006, effective Dec. 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-10.140 Electronic Ballot Tabulation—Counting Preparation and Logic and Accuracy Testing (DREs and Precinct Counters)

PURPOSE: This rule provides procedures in connection with the preparation of Direct Recording Electronic voting systems (DREs) and Optical Scan Precinct Count voting systems (Precinct Counters) for vote recording and tabulation, including equipment and program preparation and pre-election logic and accuracy testing and certification.

(1) Election authorities in jurisdictions in which direct recording electronic (DREs) or Precinct Counters are used shall be responsible for ensuring that the devices accurately record and count all proper votes cast and that the systems comply with all applicable state statutes and rules.

(2) The election authority shall be responsible for taking all steps necessary to ensure that the DREs and Precinct Counters operate properly at the time of the pre-election public logic and accuracy test and during the tabulation of votes on the day of the election.

(3) The election authority shall be responsible for making necessary arrangements for a backup ballot tabulating method.

(4) The election authority shall be responsible for providing a duplicate of the counting program for the computer system on which the ballot tabulation is to be done, regardless of the backup counting system used.

(5) The election authority shall be responsible for appointing a bipartisan accuracy certification team(s) pursuant to 15 CSR 30-10.040(5) and (6).

(6) Prior to election day the election authority shall supervise a public logic and accuracy test of the DREs and Precinct Counters conducted by the accuracy certification team(s).

(A) The logic and accuracy test shall be open to any member of the public, and the election authority, by some appropriate method, shall notify the public of the time and date of the test.

(B) Persons, other than candidates and other individuals required to be notified under section 115.233, RSMo, wishing to participate in the testing process, in the manner provided in state law and this rule, shall file a written request with the election authority at least twenty-four (24) hours prior to the publicized beginning of the logic and accuracy test.

(C) The election authority shall cause each DRE and Precinct Counter to be programmed for the ballot style for the precinct(s) at which the DRE or Precinct Counter will be used and the programmed memory card assigned to that unit shall be inserted. After programming the DREs and Precinct Counters, each unit shall have such internal diagnostic tests performed as shall be directed by the election authority. Following the completion of the diagnostic tests, all units shall have an internal logic and accuracy test performed using the programmed ballot style for the election and precinct(s) for which the unit is being prepared and shall test the conditions described in 15 CSR 30-10.040(7)(C). In addition, for DREs and electronically-assisted ballot marking devices, the test script shall include votes cast using a combination of audio and touch-screen methods.

(D) The accuracy certification team(s) shall compare the results of the electronic test to the data entered and to the results from a manual count of the paper cast vote records for the DREs and the results of a manual count of the optical scan paper ballots for the Precinct Counters. If the results are incorrect, then changes or corrections will be made to the programming until an errorless count is made. A unit shall not be used on election day until an errorless count is made on that unit.

AMERICAN OVERSIGHT

(E) After the team(s) is satisfied that the equipment is tabulating the votes properly, each candidate on the ballot or any representative of a group which has notified the election authority pursuant to 15 CSR 30-10.140(6)(B) may inspect the paper audit trail for the DRE and inspect and manually recount the optical scan test deck.

(F) If any unit fails any of the diagnostic or logic and accuracy tests, the unit shall not be used in an election until such unit is repaired, reprogrammed and inspected and found capable of proper functioning and passes the diagnostic and logic and accuracy tests. Upon the successful completion of the logic and accuracy test, the counters shall be cleared of any accumulated vote totals for the election and a zero tape run to verify that the vote registers in the unit are set at zero. The accuracy certification team(s) shall verify that the vote registers are set at zero and make a corresponding notation on the certification form to document the successful logic and accuracy testing and the unit shall be configured for voting. The memory card shall be sealed into the unit to prevent unauthorized access using a controlled serialized seal that is tamper resistant and resistant to inadvertent breakage and the unit shall then be securely closed in its case and a numbered seal placed on its case such that the case may not be opened until and unless the seal is broken. If the unit does not have a case, the unit shall be sealed with a numbered seal placed on the unit such that the unit may not be used for voting until and unless the seal is broken. The numbers on the seals shall be entered into verifiable seal logs.

(G) The election authority shall make a certification for each DRE and Precinct Counter stating the serial number of the unit, the number on the system counter of the unit, the number on the seal with which the unit is sealed, and that the election counter and each vote register on the unit was set at zero. The case shall be appropriately labeled with the name of the polling location in which the unit is to be used and the serial number of the unit. The certification shall be retained with the records for such election and shall be stored for the same period of time and in the same manner as required by law for other election records.

(H) All logic and accuracy test materials shall be sealed in a tamperproof container securely sealed in such a manner that if the container is opened, the seal will be broken beyond repair. All members of the accuracy certification team(s) shall verify, by signature or initials, the date and time the container was sealed on a certificate placed on the outside of the container. The election authority shall have custody of the logic and accuracy test materials, including the program, until called for by the accuracy certification team.

(I) After being prepared for voting, each DRE and Precinct Counter shall be safely and securely stored until such time as the unit is transported to the polling location in which such unit is to be used.

AUTHORITY: section 115.225, RSMo Supp. 2005. Emergency rule filed June 21, 2006, effective July 1, 2006, expired Feb. 22, 2007. Original rule filed June 21, 2006, effective Dec. 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-10.150 Closing Polling Places (DREs and Precinct Counters)

PURPOSE: This rule provides procedures for administering and closing polling places using Optical Scan Precinct Count voting systems (Precinct Counters) and Direct Recording Electronic voting systems (DREs).

(1) Once one (1) vote is cast on a DRE, the poll workers shall encourage voters to cast their votes on that unit so that at least two (2) more ballots are cast on that unit, even if not by voters needing its accessibility components, in order to protect the privacy of the voter.

(2) Abandoned Ballots.

(A) If a voter leaves the polling place after making their selections on a DRE and printing their ballot, but the voter has not cast the ballot, a bipartisan team of two (2) election judges shall cast the ballot.

(B) If a voter leaves the polling place after making their selections on a DRE, but the voter has not printed or cast their ballot, a bipartisan team of two (2) election judges shall cancel the ballot and make a corresponding notation on an Abandoned Ballot Tracking Form, initialed by both judges.

(C) If a voter places an optical scan ballot into a Precinct Counter and the Precinct Counter rejects the ballot after the voter has left the polling place and if the ballot is still in the Precinct Counter, a bipartisan team of election judges shall take action to ensure that the ballot is counted and deposited in the ballot box.

(D) If a voter leaves their optical scan ballot anywhere in the polling place other than in the Precinct Counter or ballot box and the voter leaves the polling place, the ballot shall not be counted. A bipartisan team of election judges shall mark the ballot "Abandoned" and place the ballot in the Spoiled Ballot Envelope. The judges shall make a corresponding notation on an Abandoned Ballot Tracking Form, initialed by both judges.

(3) Immediately after the polls close and the last voter has voted, the election judges shall close, or supervise the closing of, each of the DREs and Precinct Counters in the polling location against further voting.

(4) The election judges shall cause each DRE and Precinct Counter to print a minimum of one (1) tape showing the number of votes cast on that unit. They shall compare the number of ballots cast as shown on the tape with the number of ballots cast as shown on the election counter of the unit and with the number of voters who signed the precinct register and for Precinct Counters with the number of ballots marked. If these numbers are not identical, the election judges shall document the discrepancy.

(5) The election judges shall accumulate the votes recorded in each unit onto paper audit trail records for the DREs as well as the electronic medium chosen by the election authority, as appropriate for the make, model, and version of the system in use.

(6) After completing the procedures in sections (3)–(5), the memory components shall be removed from any unit that will not be returned to the central location on election night or shall remain sealed in any unit that will be returned to the central location, as appropriate for the make, model and version of the system in use. The DREs and Precinct Counters shall be turned off and secured in their cases and locked or resealed. The number of each seal shall be entered on the appropriate form along with the serial number of the unit or unit case on which it is used. The units or cases shall then be secured.

(7) Any provisional ballots, optical scan ballots, spoiled ballots, paper cast vote records and memory components shall be secured in tamperproof containers securely sealed in such a manner that if the container is opened, the seal will be broken beyond repair.

(8) Audit trail tapes, voter access cards, supervisor's card, ballot encoder devices, precinct binders, numbered lists of voters, voter certificates, recap sheets, and other such paperwork shall be transported to the election authority. In the event the paper cast vote record is unreadable, the audit trail tapes shall be available as an official record when a manual recount of votes is ordered.

AMERICAN OVERSIGHT MO-SOS-23-0911-A-000533

(9) All paper cast vote records shall be preserved and secured by election judges in the same manner as paper ballots and shall be available as an official record when a manual recount of votes is ordered and for the post-election verification of the electronically tabulated vote results required by 15 CSR 30-10.060.

AUTHORITY: section 115.225, RSMo Supp. 2005. Emergency rule filed June 21, 2006, effective July 1, 2006, expired Feb. 22, 2007. Original rule filed June 21, 2006, effective Dec. 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

15 CSR 30-10.160 Electronic Ballot Tabulation—Election Procedures (DREs and Precinct Counters)

PURPOSE: This rule provides procedures to be used by election authorities using Optical Scan Precinct Count voting systems (Precinct Counters) and Direct Recording Electronic (DREs) voting systems for securing and tabulating election results at the central location.

(1) Each unit or case shall only be opened in the presence of a bipartisan team which shall verify the accuracy of the seal number before the seal is broken.

(2) The election authority shall be responsible for ensuring that sufficient certificates or log entries are made on each transfer of DREs, Precinct Counters, memory components, paper cast vote records and ballots to accurately recreate each movement of the DRE, Precinct Counter, memory components, paper cast vote records and ballots. Each transfer shall include a statement that no election material was added, subtracted or altered except as provided by statute or rule and that no irregularities were noticed unless otherwise noted.

(3) The election authority or his/her representative shall be on hand at all times in the counting center when the ballots, paper cast vote records and memory components are unsealed. The units and containers shall be unsealed in the presence of bipartisan teams which shall verify that the seal is intact, and verify the seal number where numbered seals are used, before the seal is broken. When sealing and unsealing the containers, the members of the bipartisan teams shall verify the seal numbers by their signatures on a log sheet designed for that purpose.

(4) The tabulation and consolidation shall be performed in public. The election authority may make reasonable rules and regulations for conduct at the tabulating center, including limiting access to the tabulation area, to ensure the security of the results and the returns and to avoid interference with the tabulating center personnel.

(5) Upon receiving the DREs, Precinct Counters, memory components, paper cast vote records and ballots, the election authority shall verify that the seals are intact, verify the seal number where numbered seals are used and that there is no evidence of tampering with the units, cases, containers or their contents.

(6) Following acceptable procedures appropriate for the make, model, and version of the DRE or Precinct Counter in use, the election authority or his/her designee shall transfer the vote totals from the memory components into the election management system for official tabulation and consolidation.

(7) Prior to certification of the election results, the accuracy certification team(s) shall tabulate the same set of votes used in the pre-election internal logic and accuracy test performed pursuant to 15 CSR 30-10.140(6)(C) on each memory component used at the polling locations to tabulate votes on DREs and Precinct Counters. This section shall not apply to any memory component on which election results are stored

(A) If the results are not identical to those produced in the pre-election test for any memory component, the team shall not certify that the unit in which that component was used was operating properly.

1. In the case of a Precinct Counter, the necessary corrections shall be made to the program until the results are identical and the ballots cast on the Precinct Counter in which the memory component was used shall be retabulated and the consolidated results corrected accordingly.

2. In the case of a DRE, the paper cast vote records produced by the unit in which the memory component was used shall be hand counted and the consolidated results corrected accordingly.

(B) If the results are identical, the team shall certify that the unit was operating properly.

(8) The paper cast vote records audit trail tapes and ballots shall be kept secured until they must be unsealed to be hand counted in the post-election verification of electronic results pursuant to 15 CSR 30-10.110 or until they must be unsealed to be hand counted when a manual recount of votes is ordered. They shall only be unsealed in the presence of bipartisan teams which shall verify that the seal is intact, before the seal is broken and which shall reseal the containers in such a manner that if the container is opened, the seal will be broken beyond repair after the post-election audit or the manual recount is complete. When sealing and unsealing the containers, the members of the bipartisan teams shall verify the seal numbers by their signatures on a log sheet designed for that purpose.

AUTHORITY: section 115.225, RSMo Supp. 2005. Emergency rule filed June 21, 2006, effective July 1, 2006, expired Feb. 22, 2007. Original rule filed June 21, 2006, effective Dec. 30, 2006.*

**Original authority: 115.225, RSMo 1977, amended 1993, 1995, 2002.*

AMERICAN OVERSIGHT

> no substantial evidence was presented to support the allegation upon which the court failed to make findings; (3) where the court fails to issue a proper conclusion of law on an isolated issue and it is clear that the movant is entitled to no relief as a matter of law and will suffer no prejudice if remand is denied; (4) there were issues that were not properly raised or are not cognizable in a post-conviction motion; and (5) the motion was insufficient.

Watts v. State, 206 S.W.3d 413, 417–18 (Mo.App. S.D.2006) (internal quotations omitted); *see also Ivory,* 211 S.W.3d at 190–91.

The first exception does not apply to the case at bar because the motion court did not make any conclusions of law, and the second exception is not applicable because the motion was denied without a hearing. The third exception is likewise inapplicable because the motion court did not merely fail to issue a conclusion of law on an isolated issue but instead failed to render any findings of fact or conclusions of law on any issue. *Day v. State,* 143 S.W.3d 690, 693 (Mo.App. W.D.2004). With regard to the remaining exceptions, certainly some of the issues raised in Appellant's *pro se* motion are either insufficiently pled or raise issues not cognizable in a post-conviction motion; however, at the very least, the amended motion sufficiently states a cognizable claim that the factual basis for his plea was insufficient to support one of his convictions, and his *pro se* motion asserts that he was not adequately informed of the sentences he would receive and did not understand the plea agreement due to a mental condition. While the State argues that those claims are refuted by the record, that is not one of the recognized reasons for not remanding a case for findings and conclusions where findings and conclusions have not been issued pursuant to Rule 24.035(j). *Watts,* 206 S.W.3d at 417–18; *see also Ivory,* 211 S.W.3d at 190–91.

"By failing to provide any findings of fact or conclusions of law, the motion court left nothing for a meaningful appellate review." *Mitchell v. State,* 192 S.W.3d 507, 510 (Mo.App. E.D.2006). "[I]f we were to furnish findings of fact and conclusions of law, we would be engaging in *de novo* review which is not permitted under Rule 24.035(k)." *Id.* The judgment is, therefore, reversed and the cause remanded for further proceedings consistent with this opinion and Rule 24.035(j).

All concur.



C. Kay DOLAN, Respondent,

and

Monica Penrose, Plaintiff,

v.

Gilbert POWERS, Defendant,

and

Teresa A. Collins, Appellant,

and

Lynn Stoppy Brackin, Defendant.

No. WD 68098.

Missouri Court of Appeals,
Western District.

Jan. 29, 2008.

Background: Disappointed candidate in county auditor election filed suit challenging the election results by seeking statutory recount. After recount, the Circuit

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000535

Court, Johnson County, John R. O'Malley, J., entered judgment declaring disappointed candidate the actual winner. Candidate who was initially named winner appealed.

Holdings: The Court of Appeals, Ronald A. Holliger, J., held that:

(1) voter intent was possible to discern from election ballots in which voters did not mark the "target area" by filling in ovals to the left of candidates' names as instructed, but

(2) candidate who was initially named winner was entitled to conduct discovery as to whether the absence of election judge's initials on certain ballots was due to mistake.

Affirmed in part, reversed in part, and remanded.

1. Elections ⇦180(4)

Voter intent was possible to discern from election ballots in which voters did not mark the "target area" by filling in ovals to the left of candidates' names as instructed, but in which they instead marked a given candidate's party to the right of each candidate's name, such that the votes were properly counted during recount in county auditor race, where the marked party listings were adjacent to candidate's name, voters casting the ballots in question had consistently marked or circled party affiliation rather than the oval "target area," and the voters did not practice strict party voting. V.A.M.S. § 115.456(2)(3)(b)b; 15 Mo.Code of State Regulations 30–9.020(3)(A).

2. Elections ⇦305(6)

Trial court's determination of whether election ballots were marked in the "target area" so as to be a legal vote under the Uniform Counting Standards (UCS) for Optical Scan Ballots was a question of law for which the Court of Appeals would review de novo. 15 Mo.Code of State Regulations 30–9.020(3)(A).

3. Elections ⇦180(1)

Election ballot in which oval to the left of one county auditor candidate's name was completely filled in as instructed and the oval next to the other candidate's name contained a small mark was not an "overvote" so as to mandate that it not be counted during recount in county auditor race, where the mark next to the other candidate's name was so small that it constituted a stray mark.

See publication Words and Phrases for other judicial constructions and definitions.

4. Evidence ⇦584(1)

"Prima facie evidence" is evidence that will establish a fact or sustain a judgment unless contradictory evidence is produced.

See publication Words and Phrases for other judicial constructions and definitions.

5. Elections ⇦291

Party challenging an election recount team's decision to count ballots uninitialed by two election judges, as required by statute, has the burden of proof to show that the absence of initials was not the result of a mistake. V.A.M.S. §§ 115.457, 115.587.

6. Elections ⇦299(4)

Candidate, who was initially named winner of county auditor election but who was ordered to give up the office after recount, was entitled to conduct discovery as to whether the absence of election judge's initials on certain ballots cast in the election was due to mistake, as determined by recount team, which was the only basis upon which the team was permitted to count the uninitialed ballots, and trial judge's personal review of the ballots

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000536

was inconclusive as to the issue. V.A.M.S. §§ 115.457, 115.587.

Jean Paul Bradshaw II, Alok Ahuja, Kansas City, KS, for Appellant.

Patrick Andrew McInerney, Kansas City, KS, for Respondent.

RONALD R. HOLLIGER, Judge.

In this election contest case we are asked to determine whether the trial court properly ruled with regard to counting certain contested ballots in an extremely close local race for county auditor of Johnson County. The results of the recount changed the initially announced result of the election. Teresa A. Collins now appeals the trial court's judgment declaring C. Kay Dolan to have been the actual winner of the race after the recount that was required by law because of the closeness of the vote. Collins argues six points on appeal, three of which are dispositive. She challenges the inclusion in the final tally of certain ballots falling into two separate classes. The first are what we will call party identification ballots. The second is a group of ballots that did not contain the initials of election place polling judges. We find that the ballots containing marks in or around the candidates' party affiliations were properly counted, as they constituted a distinguishing mark adjacent to the candidate name. However, we believe that the trial court was without sufficient evidence to decide whether the absence of the statutorily mandated judge's initials was due to mistake and, therefore, remand on this point. Therefore, the judgment is affirmed in part and reversed in part.

Statement of Facts

The general election for Johnson County, Missouri, Auditor was held on November 7, 2006, and Teresa A. Collins was declared the winner by a margin of four votes. Her opponent, C. Kay Dolan, filed this suit challenging the election results pursuant to section 115.601.1.[1] After a hearing on January 3, the court ordered that a hand recount be conducted of all ballots cast using optical scanning equipment,[2] and thereafter issued a Writ of Recount pursuant to Section 115.585[3] and Section 115.587[4] setting out the specifics of how the recount would be conducted.

1. All statutory citations are to RSMo 2000 unless otherwise stated. Section 115.601.1 states that "[a]ny contestant in a primary or other election contest who was defeated by less than one percent of the votes cast for the office ... shall have the right to a recount of the votes cast for the office."

2. The court did not deem a hand recount necessary for the touch screen ballots.

3. "Whenever a recount is ordered pursuant to section ... 115.601, the court ... trying the contest shall issue a writ to each election authority responsible for conducting the election in any area in which an alleged irregularity occurred, commanding the election authority to prepare its office and all records and material relating to the contested election for the recount." Section 115.585.1.

4. "Whenever a recount is ordered pursuant to section ... 115.601, the court ... shall determine the number of persons necessary to assist with the recount and shall appoint such persons equally from lists submitted to the court ... by the contestant and the contestee.... Each recount shall be completed under the supervision of the court ... and the persons appointed to assist with the recount shall perform such duties as the court ... shall direct. Upon completion of any duties prescribed by the court ... the persons appointed to assist with the recount shall make a written and signed report of their findings to the court...." Section 115.587. "These findings shall be prima facie evidence of the facts stated therein, but any person present at the examination of the votes may be heard as a witness to contradict the findings." *Id.*

AMERICAN OVERSIGHT MO-SOS-23-0911-A-000537

The day after the conclusion of the recount, Gilbert Powers, the Johnson County, Missouri, County Clerk, submitted his Report of Findings to the court. The report concluded that Dolan, not Collins as originally announced, had won the race by a three-vote margin. The report also identified twenty-one challenged ballots, of which, three ballots were challenged by the statutory recount "team," a "team member" challenged eleven ballots, and an "observer" challenged seven ballots. Of the twenty-one challenged ballots, Respondent Powers counted eighteen ballots in reaching the recount result: fourteen for Dolan and four for Collins. After a hearing on the challenged ballots, the court found that Dolan won the election by two votes, concluding that the recount team should not have counted one of the ballots.

On February 27, the court entered its amended order/judgment, which memorialized its rulings on the challenged ballots and declared Dolan the winner of the Auditor's race. It also ordered Collins to give up the office of County Auditor.

Collins argues six points on appeal. In points I, II and IV she attacks the court's counting of Ballot numbers 22, 23, 25, 26, 29, and 30 on the grounds, variously, that the court misapplied the law, failed to apply the law, or that the judgment violated the statewide, uniform counting standards required by the equal protection clause. These are the so-called party affiliation ballots. In point III, she makes an additional attack on the counting of ballot number 22, asserting that it should have been held to be an invalid overvote. Alternatively, she argues that if the standard applied to number 22 was correct, the court should have also counted ballot number 11. Three points are dispositive and, therefore, will be addressed below.

In her first point on appeal, Collins argues that ballots containing a circle around the candidate's party affiliation should not have been counted because those ballots did not contain a mark in the "target area" of the ballot. In her fifth point, Collins argues that the court erred in counting eleven ballots as valid votes because those ballots contained no authenticating initials of the election judges as required by statute.[5] In her sixth point, Collins argues that the trial court erred in not permitting her to conduct discovery concerning the challenged ballots that did not contain the initials of the election judges.

Missouri Secretary of State's Uniform Counting Standards

The parties agree that the Missouri Secretary of State's Uniform Counting Standards for Optical Scan Ballots (UCS), published at 15 CSR 30–9.020, as well as Chapter 115 of the Missouri Revised Statutes, direct the outcome of the case.

The national drive to develop specific, uniform, statewide standards for counting mismarked ballots in close elections began with the Supreme Court's decision in *Bush v. Gore,* 531 U.S. 98, 121 S.Ct. 525, 148 L.Ed.2d 388 (2000), and the Florida election recount which spawned that decision. *Bush* vacated a Florida Supreme Court decision, which had ordered a partial recount of punch-card ballots in the 2000 presidential election. The Florida Supreme Court had ordered recount teams to determine whether additional "legal votes" existed among the ballots that tabulating machines had not counted; a "legal vote" was defined as "one in which there is a 'clear indication of the intent of the voter.' " *Id.* at 102, 121 S.Ct. 525. The Supreme Court held that conducting a recount under this amorphous standard

5. *See* section 115.457.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000538

would deny voters equal protection of the laws. *Id.* at 103, 121 S.Ct. 525. The Court held that equal protection guarantees applied not only to the right to vote, but also to the manner in which the franchise is exercised. *Id.* at 104–05, 121 S.Ct. 525. Therefore, equal protection demands that ballots be considered according to specific, uniform, statewide standards, beyond vague directives to determine "the intent of the voter." *Id.* at 105–06, 121 S.Ct. 525.

In the aftermath of the 2000 election and *Bush*, the United States Congress enacted the "Help America Vote Act" (HAVA), which contains detailed extensive provisions designed to upgrade and modernize voting equipment and election processes throughout the country. HAVA required that "[e]ach State" adopt "uniform and nondiscriminatory standards that define what constitutes a vote and what will be counted as a vote for each category of voting system used in the State." 42 U.S.C. § 15481(a)(6). Missouri Secretary of State Robin Carnahan responded to this HAVA command by reviewing and substantially revising Missouri's UCS. The UCS are tailored to each type of voting system used within the State, and are accompanied by illustrations intended to provide further specific guidance to persons called upon to determine the legality of individual ballots.

Party Affiliation Ballots

[1] Despite the instruction at the top of the ballot stating that "To vote, darken the oval(s) completely next to your choice(s), like this: [example]" [6] six voters made marks in, over, or around the candidate's party affiliation to the right of the candidate's name on the ballot, rather than in the oval to the left of the candidate's name. The recount team counted all six party affiliation ballots in Dolan's favor. The court counted all but one in Dolan's favor.[7] On appeal, Collins argues that none of these ballots should have been counted because they did not contain a mark in the "target area" of the ballot nor did they have a circle around the name of the voter's preferred candidate. She argues that these are the only two options that the UCS provides and that when promulgating the UCS, the Secretary of State expressly considered and rejected counting ballots with marks placed over the candidate's party name. As support for that position, she points to the fact that the proposed rule contained such an inclusion, which was ultimately not incorporated into the UCS.

[2] The parties disagree as to the standard of review with regard to the trial court's determination of whether these ballots were marked in the "target area." Collins argues that it is a question of application of the law, which we review *de novo*. *See Dudley v. Agniel*, 207 S.W.3d 617, 618 (Mo. banc 2006). Dolan argues that it is a question of fact, which we review under the standard of *Murphy v. Carron*, 536 S.W.2d 30 (Mo. banc 1976). Dolan argues that there is no definition of target area in the UCS and, therefore, it was a factual question as to what the target area was. We disagree. To hold that the question was merely one of fact would undermine the statutory and constitutional requirement of a uniform statewide counting standard. Nevertheless, we likewise do not accept Collins' argument that the statutes

6. An appendix to this opinion includes one of the contested "party affiliation ballots" for illustration.

7. The court did not count one ballot on which only the "D" in "DEM" was colored in because it could not "ascertain what the person intended."

AMERICAN OVERSIGHT

and regulations define a proper ballot as being only one that has a mark in the oval. The oval is the "target area" as Collins contends. *See* 15 CSR 30–9.020(3)(A). However, the regulation does not limit the definition of a proper mark to one that is in the oval. In full, the regulation establishes:

> The following marks shall be considered expressions of voter intent: (A) Any ballot which is properly marked in the target area as specified by the ballot instructions. (B) [not relevant here]. (C) The target area next to a candidate or issue preference is circled. (D) There is a distinguishing mark in the target area next to a candidate or issue preference issue, including but not limited to the following examples: [exemplar ballots and marks set out in the regulation]. (E) The name of a candidate or issue preference is circled. (F) [not relevant here].

15 CSR 30–9.020(3). In essence, Collins contends that if a ballot is not marked as shown in one of the examples illustrated in the regulation, it cannot be considered indicative of voter intent. We disagree with her conclusion and do not believe that either the Missouri General Assembly or the UCS intended that result.

Dolan argues that the examples set out in subsection (D) are by their own terms not exclusive. Although correct, we do not agree with Dolan that this subsection creates a different definition of target area. We believe that Collins correctly argues that subsection (D) only applies to various methods of marking (other than filling in) the target area, which in the case in question is the oval. That agreement with Collins' argument does not mean, however, that the trial court erred.

We must also be guided by the instructions given by the legislature in Chapter 115 of the Missouri Revised Statutes at the same time that it directed the Secretary of State to develop the regulations being discussed. Under the section titled "Counting of Votes" the election authority is given specific standards of how to count votes depending on which type of system is used to cast the ballot. For counting ballots cast using optical scan voting systems (the system in question here), it is directed that:

> "In jurisdictions using centrally based tabulators, if a ballot is so rejected it shall be reviewed by a bipartisan team using the following criteria:
>
> . . .
>
> (b) Voter intent shall be determined using the following criteria:
>
> a. There is a distinguishing mark in the printed oval or divided arrow adjacent to the name of the candidate or issue preference. [This provision is incorporated and explained in subsections (A) and (C) and (D) of the regulation as discussed above.]
>
> b. There is a distinguishing mark ***adjacent*** *to the name of the candidate* or issue preference": or
>
> c. The name of candidate or issue preference is circled. [This provision is incorporated and explained in subsection (E) of the regulation.]

Section 115.456.2(3)(b)b (2006 Cum.Supp.) (emphasis added).

There is no portion of the regulation that sets out or explains subsection b. of the statute. To accept Collins' argument would force us to conclude that subsection b. has no meaning because it is not incorporated into the UCS by the Secretary of State. We cannot assume the legislature intended a meaningless act. *Wollard v. City of Kansas City,* 831 S.W.2d 200, 203 (Mo. banc 1992). It is this provision of the statute that we will consider in determin-

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000540

ing whether the election judges and the trial court erred in applying it to the ballots in question.[8]

Here, the court counted five ballots (numbers 22, 23, 25, 26 and 30) in which marks were made in, over, or around the candidate's party affiliation to the far right-hand side of the ballot, rather than in the oval immediately to the left of the candidate's name. The definition of "adjacent" is "[l]ying near or close to; sometimes, contiguous; neighboring." BLACK'S LAW DICTIONARY 41 (6th ed.1990). A mark made in, over, or around the candidate's party affiliation, which is to the right of the party's name is sufficient to satisfy the "adjacent to" requirement of Section 115.456.2(3)(b)b. It is particularly noteworthy that the voters casting the ballots in question had consistently marked or circled each candidate's party affiliation, and had voted for candidates from differing parties. Nevertheless, Collins argues that the ballots were improperly counted because they violated the last clause of section 115.456.5 that "[n]otwithstanding any other provisions of law, a distinguishing mark indicating a general preference for or against candidates of one political party shall not be considered a vote for or against any specific candidate." We agree with Dolan that the use of the singular term "mark" along with the phrase "indicating a general preference" is a prohibition against strict party voting. The legislature's intent to prohibit voting by way of a "straight party ticket" is also evident from section 115.237, which prohibits the election authority from designing a ballot that allows "a person to vote a straight political party ticket." Section 115.237.4.

Separate Challenge to Ballot Number 22

[3] Collins separately challenges ballot number 22 on an additional ground. She contends that it should not have been counted in favor of Dolan because it was an overvote. Alternatively, she argues that if it was properly counted then ballot number 11 in favor of Collins was improperly and inconsistently rejected as an overvote. An overvote occurs when a ballot is marked for more than one candidate in the same race. Overvotes are not to be counted. Section 115. 453(2). On ballot number 22, the oval next to Dolan's name was completely filled in while there was a small mark in the oval next to Collins' name. The court found that the mark in the oval next to Collins' name was so small that it appeared to be infinitesimal and a stray mark. Collins now argues that, under the statute and the regulation, both marks are distinguishing marks indicating a vote for both candidates. She argues again that, under regulations, no example is given permitting such an action. She also relies on the fact that, in her final regulation, the Secretary of State omitted a provision in the proposed rule that would have allowed hesitation or stray marks to be considered an expression of voter intent. The examples given in 15 CSR–30.9.020(F) are for situations where the voter has clearly and expressly made a distinguishing mark that would otherwise be sufficient to be counted as a vote for both parties in the race. She has turned this example on its head and contradictorily argues that a hesitation or stray mark on ballot 22 should be counted as a vote for her. This is the position rejected apparently by the Secretary in adopting the final regulations. Moreover, all of the examples set forth in the UCS

8. Collins also argues that the Secretary of State specifically rejected a proposed regulation that would allow for counting votes with a mark on the party affiliation next to the candidate's name. We need not answer that argument because we are bound by the statutes as well as the regulations in determining the question of voter intent.

AMERICAN OVERSIGHT

deal with situations where a clear overvote has been cast and some other marking is used to determine which mark should be counted. Nor do we accept Collins' argument that consistency would also require counting ballot 11 in her favor under the standard applied by the court. Ballot number 11 contains an oval completely filled in for Collins. The oval next to Dolan's name contains a mark that fills nearly 25% of the oval and extends beyond its boundary. It is not a stray or hesitation mark and would clearly be sufficient to constitute a "distinguishing mark" for a candidate. It was clearly an overvote under the statutory standard. Ballot number 22 was not.

In conclusion, we find that the trial court correctly counted ballots 22, 23, 25, 26, and 30 for candidate Dolan. Its ruling and judgment comport with the statutes, UCS, and the requirements of equal protection. The court did not apply personal and subjective tests in determining voter intent. Points I, II, III, and IV are denied.

Because the counting of these ballots does not definitively determine the results of the election from the recounts, we must consider the challenges to the other class of ballots.

Non-initialed Ballots

During the recount, Respondent Powers and the recount team counted eleven ballots that were not initialed by the election judges as required by statute. These ballots were marked seven to four in favor of Dolan. Section 115.457 provides that "[i]f a ballot appears without the initials of two election judges, the ballot shall be rejected, except when it appears the absence of initials is due to mistake of the election judges and that the ballot is otherwise legal and proper." The court held that the unauthenticated ballots should be counted in the absence of evidence of "some sort of obvious irregularity." Collins argued that she should have been permitted to conduct "very limited discovery" into the circumstances surrounding the absence of the required election judges' initials. The court denied this request.

A quick outline of the voting procedures will assist us in our analysis. A voter entering a polling place first signs the precinct register, and two election judges of opposing political parties identify the voter and initial the register. Section 115.431 (2006 Cum.Supp.). "All voter's names on the precinct register [are] numbered consecutively in the order in which they have signed . . ." Section 115.431 (2006 Cum.Supp.). After the voter's identity has been certified, "two judges of different political parties, or one judge from a major political party and one judge with no political affiliation, shall . . . initial the voter's ballot or ballot card." Section 115.433 (2006 Cum.Supp.). Once these requirements have been satisfied, "the election judges shall allow the voter to proceed to the voting booth and vote." Section 115.435.

Immediately after the polls close "in each polling place using an electronic voting system, the election judges shall secure the marking devices against further voting" [9] and "remove the ballot cards from the ballot box and separate the ballots with write-in votes from those without write-in votes." [10] Section 115.467.1 & .2.

9. A "marking device" is defined as "either an apparatus in which ballots are inserted and voted by use of a punch apparatus, or any approved device that will enable the votes to be counted by automatic tabulating equipment." Section 115.013(14) (2006 Cum. Supp.).

10. The election judges count the write-in votes first. Section 115.467.1.

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000542

"All ballot cards shall be counted in order by polling place." Section 115.477.2. A return shall be produced by the automatic tabulating equipment [11] "showing the total number of votes cast for each candidate ... at each polling place and in the jurisdiction as a whole." Section 115.477.2.

The election judges must "[c]ertify in the tally book: the number of ballots cast by reconciling the ballot stubs against the number of identification certificates signed; the number of defective and spoiled ballots; the number of ballots with write-in votes; and the number of ballots received at the polling place which were not cast at the election." Section 115.471(1). Importantly, "[i]f the number of signed identification certificates is not the same as the number of ballots cast, the judges shall make a signed statement of the fact and the reasons therefor, if known, and shall return the statement with the statement of returns." *Id.* "The final and correct return printed by the automatic tabulating equipment added to the write-in, absentee and hand counted votes shall be the official return of each polling place and jurisdiction." Section 115.481. "As soon as practicable after each election, the election authority shall convene a verification board to verify the count and certify the results of the election." Section 115.497. "[T]he verification board shall meet and check the addition and figures on all tally sheets and statement of returns and shall compare its records with the returns made by the election judges and the election authority the day of the election." Section 115.501. The verification board must then "issue a statement announcing the results of each election held within its jurisdiction and shall certify the returns to each political subdivision and special district submitting a candidate ... at the election." Section 115.507.1 (2006 Cum.Supp.).

Section 115.457 instructs the counting judges not to count ballots in which no judge's initials appear, "*except when it appears the absence of initials is due to mistake of the election judges and that the ballot is otherwise legal and proper.*" Here, the counting judges (actually the recount team) counted the ballots; therefore, they must have decided that the exception applied.

Collins argues that Dolan, as the proponent of the non-initialed ballots, has the burden of proof to show that the absence of the initials on the eleven ballots was due to mistake of the polling judges. We disagree. Collins has failed to consider the procedural posture before the trial court after the recount was concluded. Dolan was entitled to a recount of the ballots for the auditor race under section 115.601 because of the closeness of the vote. No proof of irregularity was required. Such a recount was ordered pursuant to sections 115.585–115.601. Collins does not raise any issue about the propriety of ordering a recount or the procedure that was utilized. Under section 115.587, the court appointed a recount team of equal members from lists submitted by Collins and Dolan. Attorneys for each candidate were allowed to be present. It was the responsibility of the recount team to consider all of the ballots in question,[12] to determine whether they should or should not be counted and to make its report through Powers to the court of its findings. Each member of the team and the attorneys for the candidates

11. "Automatic tabulating equipment" is defined as "the apparatus necessary to examine and automatically count votes, and the data processing machines which are used for counting votes and tabulating results." Section 115.013(1) (2006 Cum.Supp.).

12. Because a hand recount was ordered, this would be all of the ballots cast in the race.

AMERICAN OVERSIGHT

were allowed to object to the determination by the recount team of whether or not a ballot should be counted. The recount team determined that each of the uninitialed ballots should be counted. Either Collins' attorney or one of the team members she proposed challenged those determinations at the time of the recount. Collins raises no issue that the ballots are improper for any reason other than the lack of initials.

[4, 5] According to Section 115.587, the findings of the recount team are to be considered "prima facie evidence of the facts stated therein." "Prima facie" as an adjective is defined as "[s]ufficient to establish a fact or raise a presumption unless disproved or rebutted <a prima facie showing>." BLACK'S LAW DICTIONARY 1228 (8th ed.1999). "Prima facie evidence" is "[e]vidence that will establish a fact or sustain a judgment unless contradictory evidence is produced." *See also Hobbs v. Dir. of Revenue*, 109 S.W.3d 220, 222 (Mo.App. E.D.2003). That the recount team decided to count the uninitialed ballots is prima facie evidence of the fact (required by section 115.587) that the lack of initials was the result of mistake. It was, therefore, sufficient to show a prima facie case for the inclusion of those ballots. A "prima facie case" is defined as "[a] party's production of enough evidence to allow the fact-trier to infer the fact at issue and rule in the party's favor." *Id.* at 222 n. 3. This principle has been utilized in a similar manner in other situations where the legislature has used the term "prima facie evidence." *See, e.g., Stadium W. Props., L.L.C. v. Johnson*, 133 S.W.3d 128 (Mo.App. W.D.2004) (applying section 140.460.1 to the recording of a tax deed as prima facie evidence of the regularity of the sale). We conclude, therefore, that the party challenging the counting of the uninitialed ballots by the recount team has the burden of proof. In this case the burden would be on Collins to show that the recount team erred in counting the ballots because the absence of initials was not the result of a mistake.

[6] Collins requested discovery on this issue, which the court denied. Instead, the court issued its judgment based on the face of the ballot. We believe that the trial court erred in this respect and that Collins should have been allowed to conduct discovery on this issue.

The most obvious purpose of the initials requirement is to prevent voting fraud perpetrated in one of two ways: casting a ballot without being properly signed-in by the polling judges, or casting more than one ballot. The statutes require the polling place judges to compare the number of signed-in voters with the number of ballots cast to detect such possible fraud. *See* section 115.471. That report is to be reviewed by the election authority and was available to the recount team. That would seem to be the first avenue for Collins to seek discovery. There may be other evidence also relevant to the issue. We reject that the trial judge's personal review of the ballots was conclusive as to the issue. Rather, it was first the recount judges who had to determine whether the absence of initials on the ballots was a mistake. Thus, the fact that they counted those ballots was prima facie evidence of mistake. The challenging party, in this case Collins, has the burden to show that the recount judges erred and should have been allowed to conduct discovery on this issue.

For the reasons stated, the determination of the trial court to count the so-called party identification ballots is affirmed and the rest of the matter reversed and remanded for discovery by Collins on the limited issue of the non-initialed ballots

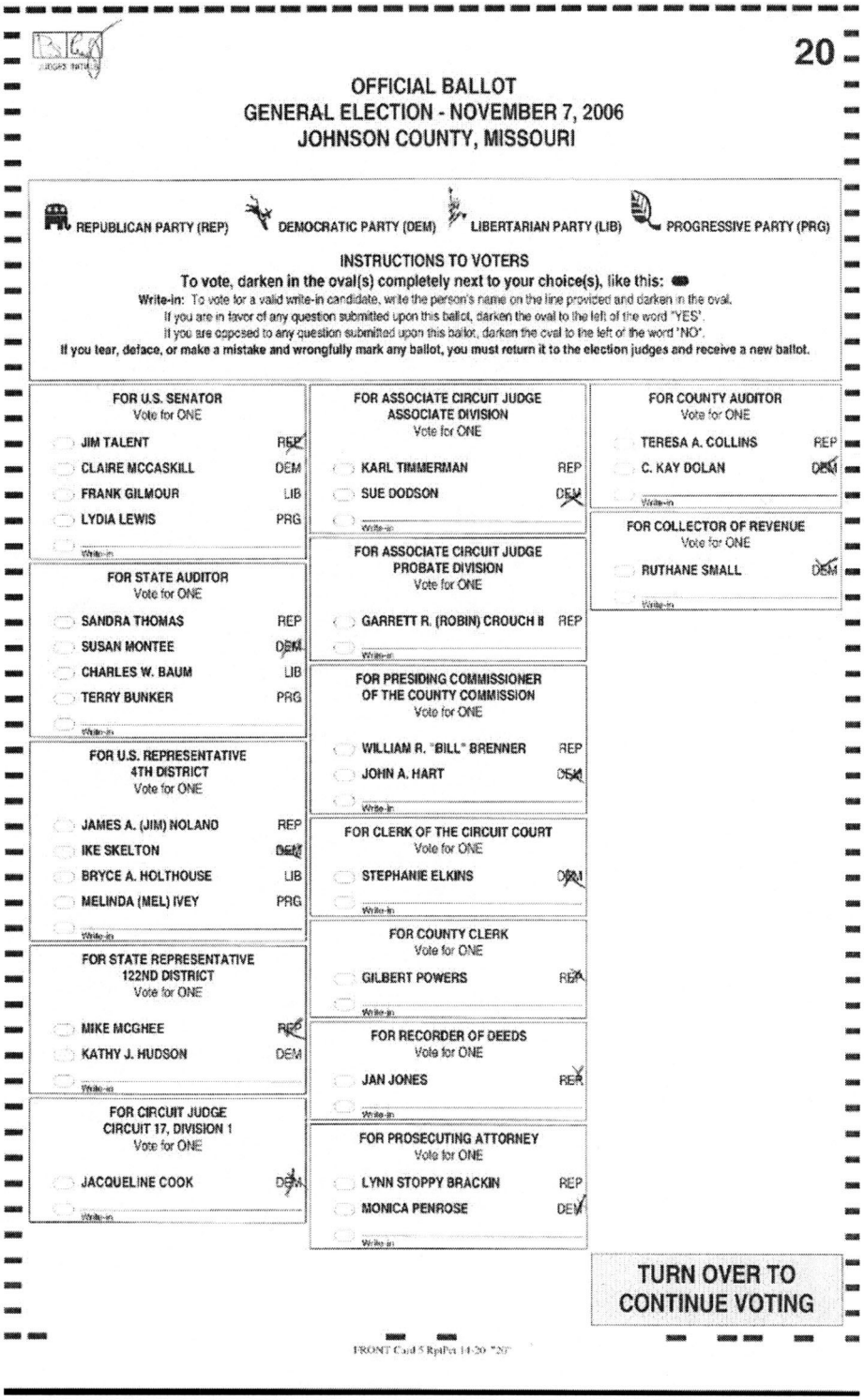
AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000544

and an evidentiary hearing by the judge on that issue in accordance with the principles enunciated in this opinion.

PATRICIA A. BRECKENRIDGE, Presiding Judge,[13] and PAUL M. SPINDEN, Judge, concur.

13. After this case was submitted for this court's decision, Judge Breckenridge was appointed to the Supreme Court of Missouri. By special assignment, she has continued to serve as a member of this court's panel in this case.

AMERICAN OVERSIGHT



20

OFFICIAL BALLOT
GENERAL ELECTION - NOVEMBER 7, 2006
JOHNSON COUNTY, MISSOURI

REPUBLICAN PARTY (REP) DEMOCRATIC PARTY (DEM) LIBERTARIAN PARTY (LIB) PROGRESSIVE PARTY (PRG)

INSTRUCTIONS TO VOTERS

To vote, darken in the oval(s) completely next to your choice(s), like this: ●

Write-in: To vote for a valid write-in candidate, write the person's name on the line provided and darken in the oval.
If you are in favor of any question submitted upon this ballot, darken the oval to the left of the word "YES".
If you are opposed to any question submitted upon this ballot, darken the oval to the left of the word "NO".
If you tear, deface, or make a mistake and wrongfully mark any ballot, you must return it to the election judges and receive a new ballot.

FOR U.S. SENATOR
Vote for ONE
- JIM TALENT REP
- CLAIRE MCCASKILL DEM
- FRANK GILMOUR LIB
- LYDIA LEWIS PRG
- Write-in

FOR STATE AUDITOR
Vote for ONE
- SANDRA THOMAS REP
- SUSAN MONTEE DEM
- CHARLES W. BAUM LIB
- TERRY BUNKER PRG
- Write-in

FOR U.S. REPRESENTATIVE 4TH DISTRICT
Vote for ONE
- JAMES A. (JIM) NOLAND REP
- IKE SKELTON DEM
- BRYCE A. HOLTHOUSE LIB
- MELINDA (MEL) IVEY PRG
- Write-in

FOR STATE REPRESENTATIVE 122ND DISTRICT
Vote for ONE
- MIKE MCGHEE REP
- KATHY J. HUDSON DEM
- Write-in

FOR CIRCUIT JUDGE CIRCUIT 17, DIVISION 1
Vote for ONE
- JACQUELINE COOK DEM
- Write-in

FOR ASSOCIATE CIRCUIT JUDGE ASSOCIATE DIVISION
Vote for ONE
- KARL TIMMERMAN REP
- SUE DODSON DEM
- Write-in

FOR ASSOCIATE CIRCUIT JUDGE PROBATE DIVISION
Vote for ONE
- GARRETT R. (ROBIN) CROUCH II REP
- Write-in

FOR PRESIDING COMMISSIONER OF THE COUNTY COMMISSION
Vote for ONE
- WILLIAM R. "BILL" BRENNER REP
- JOHN A. HART DEM
- Write-in

FOR CLERK OF THE CIRCUIT COURT
Vote for ONE
- STEPHANIE ELKINS DEM
- Write-in

FOR COUNTY CLERK
Vote for ONE
- GILBERT POWERS REP
- Write-in

FOR RECORDER OF DEEDS
Vote for ONE
- JAN JONES REP
- Write-in

FOR PROSECUTING ATTORNEY
Vote for ONE
- LYNN STOPPY BRACKIN REP
- MONICA PENROSE DEM
- Write-in

FOR COUNTY AUDITOR
Vote for ONE
- TERESA A. COLLINS REP
- C. KAY DOLAN DEM
- Write-in

FOR COLLECTOR OF REVENUE
Vote for ONE
- RUTHANE SMALL DEM
- Write-in

TURN OVER TO CONTINUE VOTING

FRONT Cnd 5 RplPct 14-20 "20"

AMERICAN OVERSIGHT
MO-SOS-23-0911-A-000546

From: acohen@nased.org
To: acohen@nased.org
Date: 12/8/2022 2:38:03 PM
Subject: Update, 12/8: NASED Call Notes, Next NASED Call is Next Friday 12/16 @ Noon ET, EAC Local Leadership Council Meeting 12/14 @ 1pmET, USPS Changes to Address Correction Notices, USPS January Price Increases, Link to Supreme Court Oral Argument, and more!
Attachments: NASED Call 12.2.22.docx

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Good afternoon, everyone!

- NASED Call:
  - Attached please find the notes from Friday's call. Our next call – and OUR LAST CALL FOR 2022!!! – will be **Friday, December 16 at noon ET**.
  - Gail Fenumiai (AK) will be retiring effective Friday. Gail is a longtime NASED member and served as NASED President in 2015. Congratulations, Gail, and thank you for your service to your voters and to all voters nationwide, as well as to our organization!
  - I know this is a time of transition for many of you, so if that describes you, please don't forget to let me know what your plans are.
- EAC:
  - The EAC will hold a Local Leadership Council meeting on Wednesday, December 14 at 1pm ET. It will be livestreamed. If you are unsure which local officials from your state serve on the council, you can find the roster here.
- USPS:
  - USPS issued a request for public comment on proposed changes to their address corrections process; the comment period ends tomorrow. The change will require Full Service and Seamless Acceptance mail customers to receive address correction notices electronically. **If a mail piece is set up with Return Service Requested, that mail piece will still be returned to you**; the only change is in the report. If you use unique serialized IMBs (ie – it's set up to allow a voter to track their individual ballot), you are either a Full Service or Seamless Acceptance mailer, so this change may impact many of you and/or your locals. This change would be effective July 9, 2023.
    - I know the public comment closes tomorrow, but it took several weeks for USPS to be able to explain this change in plain language. I'm sorry for the delay, but the notice was extremely difficult for me to understand and I didn't want anyone to get riled up.
  - The Postal Regulatory Commission (PRC) announced their proposed price increases that will take effect January 22, 2023. These price changes have already been approved by the USPS Board of Governors. For more information than you probably want, you can view the PRC filing here. As a reminder, in July 2021, the NASED Executive Board submitted a public comment requesting clarity in the schedule, frequency, and magnitude of postal rate price increases. Increases are now done on a regular schedule of January and July and are of a relatively predictable size (consumer price index plus a few other USPS-specific factors). At a high-level, January's changes are below, but remember that different factors can decrease the cost per piece of any individual mailing.
    - First Class Letters (1 ounce) - $0.60 à $0.63
    - First Class Domestic Postcards - $0.44 à $0.48
- Supreme Court:
  - Yesterday, the Supreme Court heard oral arguments in Moore v. Harper, the "independent state legislature theory" case. If you missed it, you can listen or view a transcript here.
- NASED Conference:
  - NASED conference registration is officially open! Join us February 16-18 in Washington, DC; February 15 will be the Government Coordinating Council meeting, which is open to all of you to attend if you wish to do so, though it is not part of the NASED conference. All state and territorial election office staff from offices in good standing with NASED are welcome to register as members and attend all member content. I hope to see many of you there!

AMERICAN OVERSIGHT

I think that's it for today!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Direct: 202-434-8972
Follow us on Twitter @NASEDorg!

The contents of this message, together with any attachments, are confidential and intended only for the use of the individual or entity to which they are addressed. If you are not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this message, or any attachment, is strictly prohibited. If you have received this message in error, please notify the original sender immediately by email and delete this message, along with any attachments, from your computer.

--
You received this message because you are subscribed to the Google Groups "All Communciations" group.
To unsubscribe from this group and stop receiving emails from it, send an email to allcomms+unsubscribe@nased.org.

AMERICAN OVERSIGHT

NASED Biweekly Call
December 2, 2022

NE: Thanks everyone for stuff on VoteRef. We sent back their check because their notarization was wrong. We asked for them to put in writing that they won't put our voter registration list online, and they haven't responded yet. Now they're looking for UOCAVA data from last 3 cycles, and we think they're trying to see if anyone tried to use a loophole to get ballots, similar to what happened in Wisconsin. [EDITOR'S NOTE: Wisconsin state law does not require military voters to register to vote.]
NV: We got the same records request from VoteRef. I don't know if what we provided satisfied them or not, but we did it with minimal effort.

NV: The new Nye County clerk decided he wanted to run a parallel process tabulating by hand in addition to the machine count, which was the official tabulation. They hand counted about 26k ballots by hand in addition to machine tabulation. His plans going forward will be to continue to this kind of hand count "audit." People only made it about four hours before their accuracy started deteriorating, but he thinks that over time, people got better. The idea is spreading, potentially to other counties. One of the arguments in favor is that it gets more people involved and informed about election processes.

MI: Activists here seem to have discovered the risk limiting audit (RLA). Maybe that will finally help people understand what we've been trying to do moving towards these kinds of audits. We've also gotten recount requests for ballot proposals that were not even in close, so we're doing a partial recount of a significant percentage of the state. We think this is possibly paid for by an out of state entity.
NV: We've had something similar. We had three ballot measures, and the smallest margin was ~55k. We're seeing a lot of requests for recounts for all of them. When we explained they had to pay the estimated costs up front, none of them have actually moved forward. They were demanding a recount conducted by hand and by a third party, which we don't permit.
NE: I have a state legislator who is requesting a recount. They wanted a hand recount, but we're not doing that. Also, we have a provision preventing recounts of ballot measures.

NV: We're looking at having only seven local election officials who will have experienced 2020, 10 new one, including four I'd consider deniers. We're struggling with professionalization.

AK: Gail is retiring effective December 9.
WY: Kai leaving the office by January 2.

AMERICAN OVERSIGHT

From: Sharon Lawrence <asksharonlawrence@gmail.com>
To: info@nased.org
Clay.helms@sos.alabama.gov
gail.fenumiai@alaska.gov
info@eo.as.gov
klorick@azsos.gov
Leslie.Bellamy@sos.arkansas.gov
jana.lean@sos.ca.gov
Judd.Choate@coloradosos.gov
administrative@votecnmi.gov.mp
ted.bromley@ct.gov
anthony.albence@delaware.gov
mevans@dcboe.org
Maria.Matthews@dos.myflorida.com
bevans@sos.ga.gov
vote@gec.guam.gov
elections@hawaii.gov
jason.hancock@sos.idaho.gov
bmatthews@elections.il.gov
bking@iec.in.gov
anussmeyer@iec.in.gov
heidi.burhans@sos.iowa.gov
Bryan.Caskey@sos.ks.gov
karen.sellers@ky.gov
Sherri.Hadskey@sos.louisiana.gov
Julie.Flynn@maine.gov
Linda.Lamone@maryland.gov
Michelle.Tassinari@sec.state.ma.us
BraterJ@michigan.gov
david.maeda@state.mn.us
kyle.kirkpatrick@sos.ms.gov
Peters, Chrissy <chrissy.peters@sos.mo.gov>
DCorson@mt.gov
wayne.bena@nebraska.gov
mwlaschin@sos.nv.gov
patricia.piecuch@sos.nh.gov
Mandy.Vigil@state.nm.us
Todd.Valentine@elections.ny.gov
Kristen.Zebrowski.Stavisky@elections.ny.gov
karen.bell@ncsbe.gov
bnewby@nd.gov
jsilrum@nd.gov
agrandjean@ohiosecretaryofstate.gov
paul.ziriax@elections.ok.gov
deborah.scroggin@oregon.gov
jesmathis@pa.gov
frosado@cee.pr.gov
rrock@sos.ri.gov
robert.rapoza@elections.ri.gov
hknapp@elections.sc.gov

AMERICAN OVERSIGHT

kea.warne@state.sd.us
suzanne.wetz@state.sd.us
Mark.Goins@tn.gov
kingram@sos.texas.gov
ryancowley@utah.gov
will.senning@vermont.gov
caroline.fawkes@vi.gov
susan.beals@elections.virginia.gov
BWestfall@wvsos.com
Meagan.Wolfe@wisconsin.gov
kai.schon@wyo.gov
nass@sso.org
lforson16@gmail.com

Date: 10/28/2022 11:22:52 AM

Subject: Voter Education Materials - Designed Especially for Distribution to the Media (For Your Use)

Attachments: Elections - 2022, Voting Tips 1a - Tips 1 to 31.pdf
Elections - 2022, Voting Tips 1b - Tips 32 to 45.pdf
Elections - 2022, Voting Tips 1c - Links.pdf
Elections - 2022, Voting Tips 1g - Races.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

For almost a decade, my consulting clients were predominantly in the elections industry (e.g., Pew's Election Reform & Information Project and Hart InterCivic). During that time, I also was engaged by the National Association of County Information Officers to write a voter education guide for county officials. As a result, I developed a passionate interest in elections and especially voter education.

Fixing What is Broken in Voter Education

As one might expect, I've been APPALLED by the attack on the integrity of the elections process, the unrelenting voter suppression efforts, and the media's inability/unwillingness to correct the record. Moreover, I was concerned with news reports that young voters aren't participating in elections because elections officials aren't using social media to connect with them and that's the only way they get information.

I resolved to do something to help. Toward that end, I've put together the attached documents. Specifically what I've done is:

1) Voting Tips - Detailing 45 tips that all voters should take to make certain they get registered to vote, THEIR VOTE COUNTS, and they have confidence in the integrity of the voting process. This information is designed in "Tip" format so that elections officers may convert each tip easily into a social media post - complete with eye catching graphics. As you'll see, examples and graphics are drawn from election offices all across the country - so that readers may appreciate how election administration is similar and/or different across the US;
2) A state-by-state breakout of the key races on the ballot this year, including Supreme Court positions; and
3) Comprehensive state-by-state links to election websites, including links to ballot tracking systems and voter guides! I'm also updating my links to state election statutes/regulations/constitutional provisions which will be finished by the weekend along with the other state-by-state data to accompany the tips.

AMERICAN OVERSIGHT

I've been posting this information on LinkedIn but I've decided that it's important to share directly with key elections leaders. For the last two years, everyone in the elections field has been so under siege, you need all the help you can get.

If you're reluctant to open an attachment, note that all the documents are posted with my LinkedIn profile (the fastest way to find them is to go to the documents tab).

Hope this helps!

--
Sharon Lawrence
PO Box 387
San Marcos, TX 78667-0387
(512) 757-8669/837-5670
AskSharonLawrence@gmail.com
https://www.linkedin.com/in/asksharonlawrence/

AMERICAN OVERSIGHT



Voting Tips

How to Make Certain Your Vote Counts in 2022

Election laws in the United States are extremely complex, increasingly so. Except for a few basic standards set by federal law, the states are free to establish their own procedures for federal, state, and local elections in their jurisdiction. To help everyone make certain they may vote in the November 2022 General Election AND that each and every vote cast on a race or a ballot issue counts, the following tips are offered.

AMERICAN OVERSIGHT

Information is provided as well to help voters understand the procedures in place so that they may have confidence in the outcome of the election.

For subjects not covered in these tips or more state specific information, check the following resources on election policies and procedures:

All States – Election Deadlines, Laws & Procedures: https://www.nass.org/can-I-vote
All States – Local Elections Officials: https://www.usvotefoundation.org/vote/eoddomestic.htm
Ballot Issues and Candidates: https://www.vote411.org/ (League of Women Voters)
Ballot Issues and Candidates: https://justfacts.votesmart.org/ (Project Vote Smart)
Military and Overseas Voters: https://www.fvap.gov/ (Federal Voting Assistance Program)
Overseas Voters: https://www.overseasvotefoundation.org/vote/home.htm
Right to Vote Restoration – Felony Convictions: https://campaignlegal.org/restoreyourvote
https://restoration.ccresourcecenter.org
Time Off to Vote: https://www.workplacefairness.org/voting-rights-time-off-work
Voting Rights: https://www.justice.gov/crt/voting-section
Youth Voters: https://www.campusvoteproject.org/
Youth Voters: https://www.rockthevote.org/

~~~~~~~~~~~~~~~~

Author's Note

No endorsements of any candidate are intended by photographs or texts in this document. The graphics were selected simply because they illustrated my point well. In the case of the cover photograph, the gentleman in the picture happens to have been a high school classmate!

Sharon Lawrence
PO Box 387
San Marcos, TX 78667-0387
(512) 757-8669
https://www.linkedin.com/in/asksharonlawrence
(Last Updated: October 27, 2022)

~ Copyright by Sharon Lawrence 2 ~

AMERICAN OVERSIGHT
~~~~~~~~~~~~~~~~



The Tips

Preface

What's at Stake in the 2022 General Election? .....

Know Who Is In Charge

#1. Identify Your State's Chief Election Official & Bookmark the Election Information Website(s) .....
#2. Identify Your Local Chief Election Official & Bookmark the Election Information Website .....

Get Ready for the Election

#3. Mark Your Calendar for This Important Deadline (Voter Registration).....
#4. Mark Your Calendar for This Important Deadline (Mail Ballot Return) .....
#5. Register to Vote If You Have Not Already Done So.....
#6. Review Your Voter Registration Certificate.....
#7. Update Your Signature On File .....
#8. Become Informed of the Special Procedures If You Are a Member of the Military or An Overseas Voter.....
#9. Investigate the Factors Affecting Where You May Vote If You Are a College Student .....
#10. Determine Residence for Voting Purposes.....
#11. Volunteer to Help Administer Elections.....
#12. Develop a Firm Grasp of the Voter Identification Requirements, If Any .....
Obtain the Necessary Documentation If You Do Not Already Possess It.....

Learn About the Candidates & the Issues on the Ballot

#13. To Know Which Races & Issues Will Be Before You, Look for a Sample Ballot .....

~ Copyright by Sharon Lawrence 3 ~

AMERICAN OVERSIGHT

#14. Learn About the Candidates (from the Candidates) .....
#15. Learn About the Candidates (from Other Sources) .....
#16. Don't Forget to Educate Yourself on the Judges/Justices Seeking Election or Retention ....
#17. Study the Issues That Will Appear on the Ballot.....
#18. Know Who is Financing the Campaigns .....

Understand the Voting Process

#19. Determine When and Where You May Vote in Person.....
#20. Determine If You May Vote Absentee/By Mail Instead .....
#21. Voting in Case of a Family or Medical Emergency .....
#22. Be Mindful of What You May or May NOT Do At the Polling Place or Near a Ballot Drop Box.....
#23. Familiarize Yourself with Write-In Procedures.....
#24. Master the Art of Marking Your Ballot Properly .....
#25. Don't Forget to Apply the Appropriate Postage!.....
#26. Pay Attention to the Restrictions on Who May Help You Vote and/or Handle Your Ballot in Any Way.....
#27. Track Your Ballot Request or Return .....
#28. Be Alert for Runoff Elections.....
#29. Understand How Ranked Choice Voting Works.....
#30. Get Informed About Election Security Measures/Participate as a Citizen Observer .....
#31. Ensure That You Are Using Only Official Election Materials.....

Know Your Rights

#32. Be Aware of Your Basic Rights as a Voter (i.e., Voter Bill of Rights).....
#33. Right to Accessible Polling Places and Voting Equipment.....
#34. Right to Bilingual Election Materials .....
#35. Right to Cast a Provisional Ballot In Case of Questions about Eligibility .....
#36. Right to Take Time Off From Work to Vote.....
#37. Right to Vote If In Line When Poll Closing Time Arrives.....
#38. Right to Vote If Incarcerated, But Not Yet Convicted .....
Right to Vote After Felony .....Conviction
#39. Right of Designated At Risk Individuals to Request That Certain Identifying Information Be Withheld from the Public .....

Know Your Responsibilities

#40. Respect the Rights of Voters and the Elections Process.....
#41. Respect the Rights of Candidates To Communicate with Voters.....
#42. Comply with Government Regulations for the Display of Campaign Signage.....
#43. Report Election Fraud or the Violation of Voting Rights.....
#44. Be Patient – Wait for Official, Certified Results .....
#45. Congratulate the Winners & Accept the Certified Election Results! .....

AMERICAN OVERSIGHT

Appendix

Appendix 1.	How Elections Work – The Basics (Arizona)	
Appendix 2.	Guidance on Polling Place Conduct & Preventing Voter Intimidation (Arizona)	
Appendix 3.	Election Security (Overview)	
	Election Security Overview (Indiana)	
	Voter Registration Cancellation Procedures (Michigan)	
Chart #1.	State & Local Election Officials, Official Election Websites, Ballot Tracking Tools & Voter Guides	
Chart #2.	Voter Registration Deadlines	TBA
Chart #3.	Mail Ballot Request Deadlines	TBA
Chart #4.	Mail Ballot Return Deadlines	TBA
Chart #5.	Polls Open – Early Voting & Election Day	TBA
Chart #6.	Residency Requirements	TBA
Chart #7.	Time Off to Vote	TBA
Chart #8.	Election Certification Deadlines	TBA

~ Copyright by Sharon Lawrence 5 ~

AMERICAN OVERSIGHT

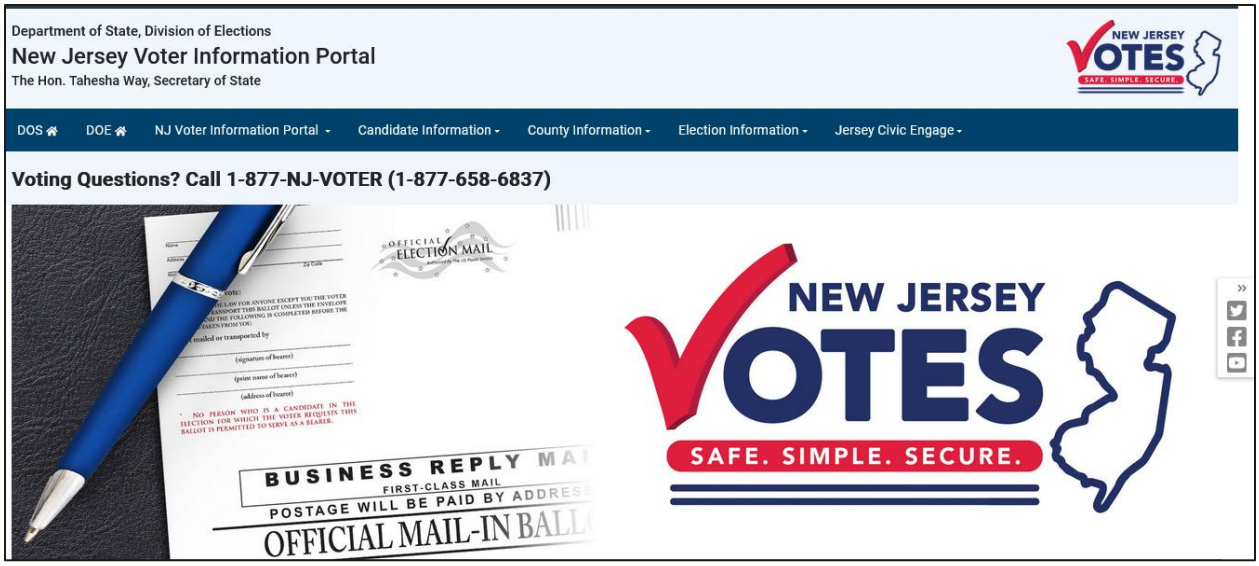


What's at Stake in the 2022 General Election?

- 435 seats in the US House of Representatives
- 33 seats in the US Senate
- 36 Governors offices
- 30 Attorney General offices
- 27 Secretary of State positions
- 6,279 state legislative seats in 46 states (plus special elections)
- 74 State Supreme Court Judgeships

~ Copyright by Sharon Lawrence 6 ~

AMERICAN OVERSIGHT



Know Who Is In Charge

Voting Tip #1
Identify Your State's Chief Election Official
Bookmark the Election Information Website(s)

Voting Tip #2
Identify Your Local Chief Election Official(s)

The titles of officials charged with the responsibility for administering and/or overseeing election administration in the states and localities vary widely across the US. At the state level, the agencies responsible may be a Board of Elections (e.g., Maryland), the Lieutenant Governor (e.g., Alaska), or the Secretary of State (e.g., Nebraska). It's wise, therefore, to check the appended chart and bookmark that entity's official website(s) for speed of future reference.

On the local level, the same diversity in allocation of responsibilities occurs. Alabama law assigns the responsibility for election administration to the Judge of the Probate Court, whereas Texas splits the responsibility for election administration typically between the County Clerk (general elections administration) and the County Tax-Assessor Collector (voter registration). See the appended chart for links to all the local elections websites.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 7 ~

Email Signup Tool

Signup today to receive important election information by email!

The Cook County Clerk's Email Signup Tool is a quick and easy way for suburban residents to receive the most up-to-date information for every election.

By signing up, voters will be sent timely and important email notifications that will not only open lines of communication with the public but also save taxpayer time, money and worry about any Election Day concerns regarding:

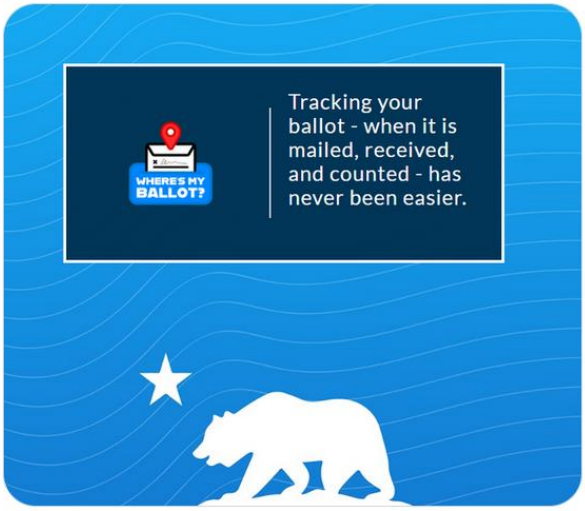
- General Election Information
- Your Official Election Mailer
- Polling Place Changes
- Election Day Information
- Cook County Clerk's Office Newsletter

Click Here to Signup!



VC Clerk Re... @VCClerk... · Oct 17

It's not too late to sign up to track your ballot. Sign up at wheresmyballot.sos.ca.gov for email, text or a voice call about your ballot.
Ballottrax will send you a notification about your ballot return status whether mailed, dropped off or voted in-person.
#venturacountyvotes



5 6

Once you locate your state and local election websites, take the opportunity (if available) to sign up for email, Facebook, text, or Twitter notices that may be sent from those offices.

~ Copyright by Sharon Lawrence 8 ~

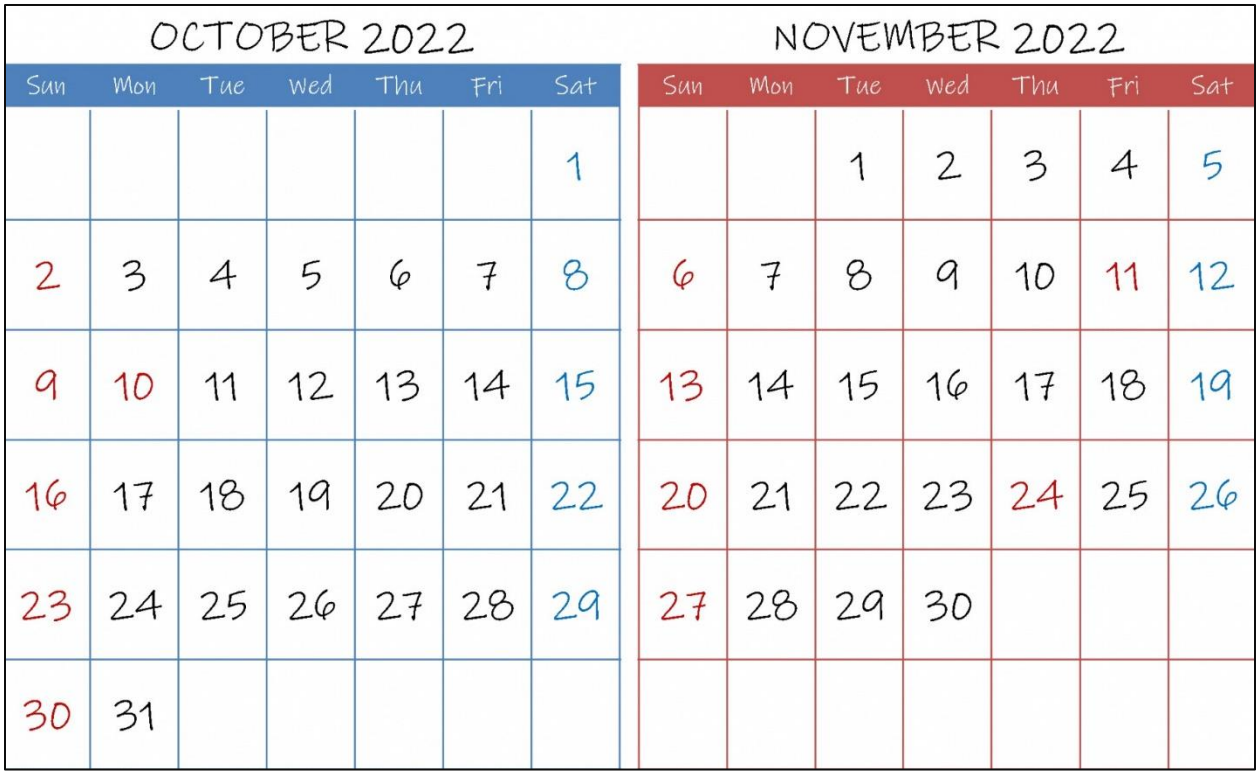
AMERICAN OVERSIGHT



Get Ready for the Election

~ Copyright by Sharon Lawrence 9 ~

AMERICAN OVERSIGHT



OCTOBER 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

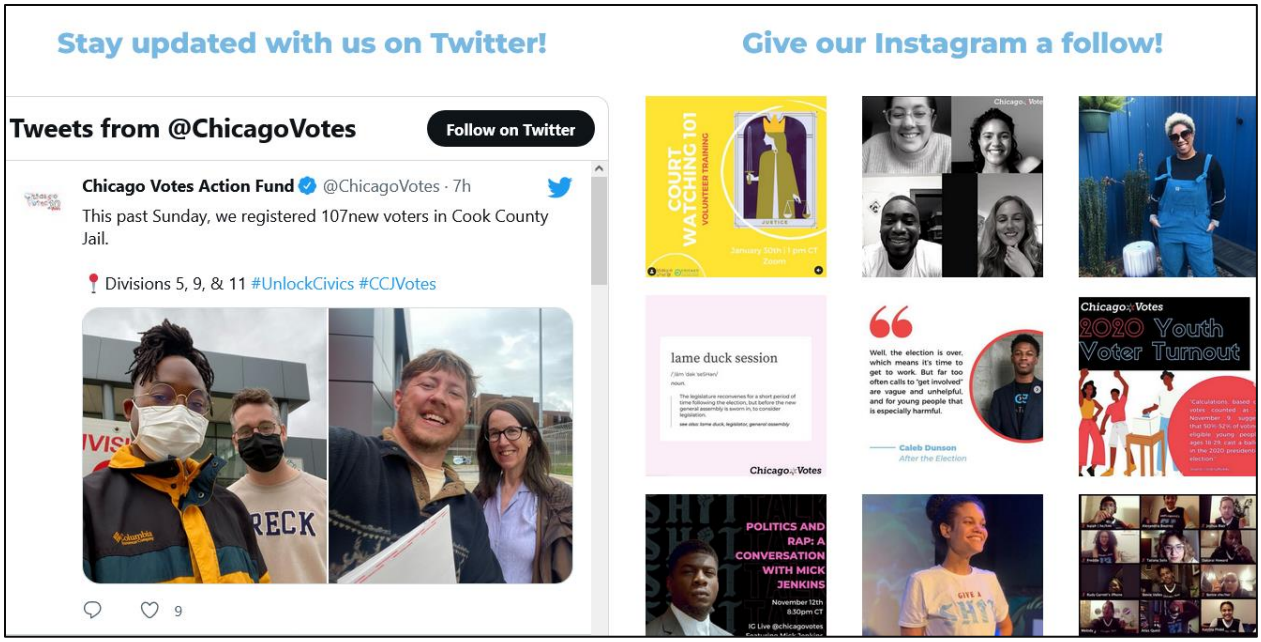
NOVEMBER 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Voting Tips #3 & #4
Mark Your Calendar for These Important Deadlines
(Voter Registration & Mail Ballot Return)

~ Copyright by Sharon Lawrence 10 ~

AMERICAN OVERSIGHT



Voting Tip #5
Register to Vote If You Have Not Already Done So

All states and territories (except North Dakota) require voters to register to vote before they are eligible to vote in an election. Procedures to complete application or update an existing one vary dramatically across the states.

An increasing number of states now allow voters to register up to and on Election Day. Others set a specific date by which a voter registration application must be received for a voter to be eligible to vote in the upcoming election.

Most make voter registration an easy process allowing for the task to be completed online. Texas is among the most prominent of states that don't allow that option except when the task is done in conjunction with a driver's license application or renewal.

~ Copyright by Sharon Lawrence 11 ~

AMERICAN OVERSIGHT



Voting Tip #6
Review Your Voter Registration Certificate

Upon a review and approval of your voter registration application, your local elections office will issue you a Voter Registration Certificate. This is an IMPORTANT document to keep in a safe place AND to have on your possession when you vote in-person. (See the graphic above for an example of the certificate used in Texas.) In addition to reporting the identification information for you (e.g., gender), the certificate lists:

- ✦ The precinct in which you must vote; and
- ✦ The Congressional/state legislative/county commissioners/city council/other districts or precincts in which you reside.

Check this document carefully when you receive it to make certain that the address and identification information is correct. If the certificate contains the word "suspense" or something similar, that's an indication there is uncertainty about your registration (e.g., current address), and your information needs to be confirmed or you need to reregister.

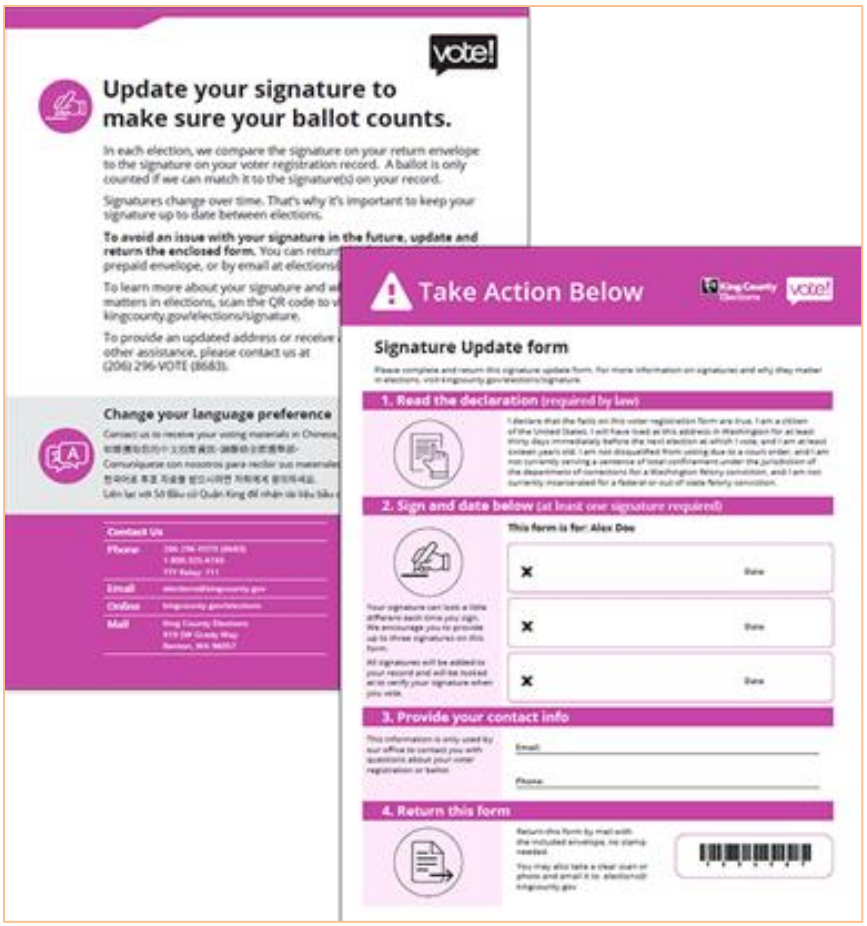
Use this document as you begin your study of candidates so that you know which races will be on your ballot. It's also handy to have with you in the voting booth or when marking your mail ballot to ensure you have the right combination of races upon which you are authorized to vote. Although

AMERICAN OVERSIGHT

elections officials strive to run error free elections, residents of six houses in a city block could have six different combinations of offices on their ballot given the nature of how boundaries for local subdivisions are drawn. Double checking is always wise.

After issuance of the initial certificate, Texas law mandates that all registered voters be mailed a new certificate in November of odd-numbered years. Other states will, no doubt, have a similar mandate to update these documents. Check the expiration date on the certificate to make certain it has not been replaced.

AMERICAN OVERSIGHT



Tip #7
Update Your Signature on File

Certain elements of the voting process (e.g., validation of a mail ballot) require the matching of a signature with the signature on file. The way we sign our name, however, changes over time. If it's been a substantial period of time since you registered to vote, it's prudent to visit the elections office to update your signature on file. The State of Washington, as shown above, has a specific form for that task.

AMERICAN OVERSIGHT



Voting Tip #8
Become Informed of the Special Procedures If You Are a Member of the Military or An Overseas Voter

For Americans who live outside the US or are serving in the military and away from home, time is of the essence to get registered, request a ballot, mark it, and return it by the deadline your state sets. That ballot return deadline may be anywhere from the close of the polls on Election Day to several days thereafter.

Some of the requisite documents may move electronically, but ballots still primarily go by snail mail. Get on this NOW! Every election administrator is required by federal law to have ballots ready 45 days before the election. For details on how to vote if you are living outside the US (e.g., Canada) and/or in the military, contact the Federal Voting Assistance Program, https://www.fvap.gov/.

AMERICAN OVERSIGHT



Voting Tip #9
Investigate the Factors Affecting Where You May Vote If You Are a College Student

College students must give careful consideration – well in advance of an election – as to where they will vote. That involves determining where they are eligible to vote and familiarizing themselves with new procedures (e.g., voter identification) if they are voting outside their home state. Idaho students are advised:

> The State Board of Education Rules Governing Residency Classification in the Idaho Administrative Code (IDAPA 08.01.04.05.08) define "domicile" as follows:
>
> "Domicile" means an individual's true, fixed, and permanent home and place of habitation; the place where the individual intends to remain and to which the individual expects to return when he leaves without intending to establish a new domicile elsewhere. The establishment of domicile in Idaho occurs when a person is physically present in Idaho primarily for purposes other than educational and can show satisfactory proof that such person is without a present intention to return to another state or acquire a domicile at some other place outside the state and the person has met any other applicable requirements of this chapter.
>
> The above-mentioned materials require that college students must establish, as with all other voter registration applicants, that the locale within which they seek to register and vote is their domicile, i.e. that they are living in the college community

~ Copyright by Sharon Lawrence 16 ~

AMERICAN OVERSIGHT

with the intention of abandoning their former domicile and with the intention of remaining permanently, or for an indefinite length of time, in the new location.

Establishing Domicile. Some of the factors which may be relevant in determining whether domicile has been established for voting purposes by a student as well as any other applicant, are as follows:

1. Has the applicant registered to vote elsewhere?
2. If married, where does his or her spouse reside?
3. Where does the applicant keep his personal property?
4. Does the applicant have any community ties to the locale he claims as his domicile – membership in church, social or service clubs, etc?
5. Where does the applicant maintain his checking and saving accounts, if any?
6. Where does the applicant pay taxes, and what address did he list as his residence on his last income tax return?
7. What is the residence listed on the applicant's driver's license?
8. If the applicant owns an automobile, where is it registered?
9. If the applicant is employed, where is his job located?
10. Does the applicant live year-round at his claimed domicile, or does he divide it elsewhere? If it is divided, how much time is spent elsewhere and for what reason?
11. What residence does the applicant list on his selective service registration, hunting or fishing licenses, insurance policies, or other official papers and documents which required a statement of residence or address.

The Virginia Department of Elections offers this guidance to college students.

How Do College Students Register to Vote in Virginia? A college student registers to vote in Virginia the same as any other applicant: every prospective voter must submit a voter registration application. Remember, you must update your voter registration information whenever you change your residence.

Every voter in Virginia must submit their residential address when registering to vote (a post office box cannot serve as a residential address). If you are unable to receive mail at your address, you must also submit a local mailing address.

A dormitory or college address can be an acceptable residential address and does not disqualify you from voting. If your local voter registration office is unable to determine your physical residency based on a college address you provided on your voter registration application, the local voter registration office will contact you to request further information needed to register you to vote. Providing your e-mail address and phone number on your voter registration application is a helpful way to ensure that the local voter registration office is able to contact you promptly. The local voter registration office may contact you by mail at the mailing address you provide on your voter registration application.

AMERICAN OVERSIGHT

What is My Residence? A prospective voter must be a resident of the Commonwealth and of the precinct where he seeks to register. In order to establish residency, a prospective voter must have a physical location where they intend to stay for an unlimited time. A person can have residency in only one place at a time.

The applicant must determine and declare their residence and may change their intent at any time.

How Do College Students Vote? A college student votes in the same manner as any other registered voter: you may vote in person on Election Day, vote early beginning 45 days ahead of an election, or vote absentee by mail.

Impact on Other Areas. Legal residence for voter registration purposes may or may not be the same as legal residence for census, driver's license, federal and state income tax, state vehicle tax, tuition, or financial aid purposes. The Department of Elections and local election officials are not trained in these complex areas. You should consult appropriate advisors regarding these issues.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 18 ~

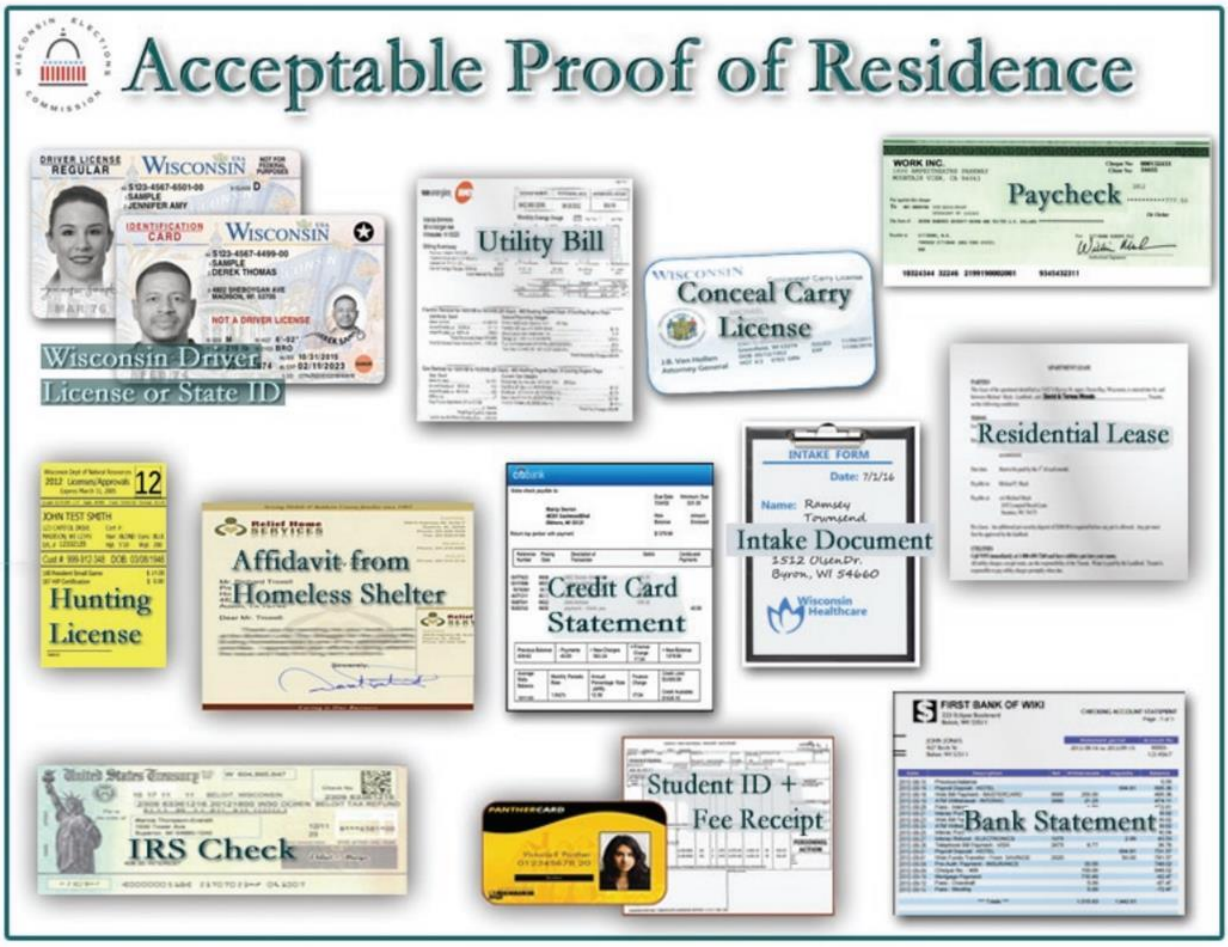


Illustration courtesy of Waterford, WI

~~~~~~~~~~~~

Voting Tip #10
Determine Residency for Voting Purposes

College students, members of the military, and the homeless are among the people who have an extra step in the voting process, i.e., they must determine what their residence is for voting purposes. Under federal law, every American citizen aged 18 or older may vote for President and Vice President, regardless of where they reside within the United States and notwithstanding any residency requirement in that jurisdiction.[1] But for state and local offices, state law governs where you may vote.

Determining Residency. Montana law Section 13-1-112, for example, sets for the following rules for determining residency:

[1] 52 U.S. Code Section 10502.

~ Copyright by Sharon Lawrence 19 ~

AMERICAN OVERSIGHT
~~~~~~~~~~~~

For registration, voting, or seeking election to the legislature, the residence of an individual must be determined by the following rules as far as they are applicable:

(1) The residence of an individual is where the individual's habitation is fixed and to which, whenever the individual is absent, the individual has the intention of returning.

(2) An individual may not gain or lose a residence while kept involuntarily at any public institution, not necessarily at public expense; as a result of being confined in any prison; or solely as a result of residing on a military reservation.

(3) (a) An individual in the armed forces of the United States may not become a resident solely as a result of being stationed at a military facility in the state.

(b) An individual may not acquire a residence solely as a result of being employed or stationed at a training or other transient camp maintained by the United States within the state.

(c) A member of a reserve component of the United States armed forces who is stationed outside of the state but who has no intent of changing residency retains resident status.

(4) An individual does not lose residence if the individual goes into another state or other district of this state for temporary purposes with the intention of returning, unless the individual exercises the election franchise in the other state or district.

(5) An individual may not gain a residence in a county if the individual comes in for temporary purposes without the intention of making that county the individual's home.

(6) If an individual moves to another state with the intention of making it the individual's residence, the individual loses residence in this state.

(7) The place where an individual's family resides is presumed to be that individual's place of residence. However, an individual who takes up or continues a residence at a place other than where the individual's family resides with the intention of remaining is a resident of the place where the individual resides.

(8) A change of residence may be made only by the act of removal joined with intent to remain in another place.

Its neighbor Washington State law defines residence in this way:[2]

"Residence" for the purpose of registering and voting means a person's permanent address where he or she physically resides and maintains his or her abode. However, no person gains residence by reason of his or her presence or loses his or her residence by reason of his or her absence:

(1) While employed in the civil or military service of the state or of the United States;

[2] Revised Code of Washington, Section 29A.04.151.

AMERICAN OVERSIGHT

(2) While engaged in the navigation of the waters of this state or the United States or the high seas;
(3) While a student at any institution of learning;
(4) While confined in any public prison.

Absence from the state on business shall not affect the question of residence of any person unless the right to vote has been claimed or exercised elsewhere.

Residency for Those Who Lack a Traditional Residential Address. States provide pathways for individuals who are temporarily or permanently homeless to vote. Washington law, for example, declares:

(1) No person registering to vote, who meets all the qualifications of a registered voter in the state of Washington, shall be disqualified because he or she lacks a traditional residential address. A voter who lacks a traditional residential address will be registered and assigned to a precinct based on the location provided.
(2) For the purposes of this section, a voter who resides in a shelter, park, motor home, marina, unmarked home, or other identifiable location that the voter deems to be his or her residence lacks a traditional address. A voter who registers under this section must provide a valid mailing address, and must still meet the requirement in Article VI, section 1 of the state Constitution that he or she live in the area for at least thirty (30) days before the election.
(3) A nontraditional residential address may be used when a voter resides on an Indian reservation or on Indian lands.
(4) A federally recognized tribe may designate one or more tribal government buildings to serve as a residential address or mailing address or both for voters living on an Indian reservation or on Indian lands. However, a voter may not use a tribally designated building as the voter's residential address if the building is in a different precinct than where the voter lives.
(5) A person who has a traditional residential address and does not reside on an Indian reservation or on Indian lands must use that address for voter registration purposes and is not eligible to register under this section.[3]

Wisconsin's Elections Commission provides this guidance to the homeless:

Homeless individuals may designate a fixed location as their residence for voting purposes if it is an identifiable location in the state of Wisconsin which could conceivably serve as a temporary residence. This location may be a homeless shelter, a park bench, or other location where a homeless individual may spend time or return to on a regular basis.

- ✦ For homeless voters, this means that if they have established a residence, they may continue to claim that residence as a voting address, even if they no longer physically reside at

[3] Revised Code of Washington, Section 29A.08.112.

AMERICAN OVERSIGHT

that location, if they have intent to return. This would allow voters who had stayed with friends or family to continue using that address for voting purposes.

- ✦ Note that P.O. Boxes are not acceptable – your voting address must be a physical location, so election officials can determine which districts you vote in, and in which contests you get to vote.
- ✦ Note that a shelter address is an acceptable residence for voting purposes, notwithstanding any restriction in the shelter's rules prohibiting its use as a residential address. "Residence" for voting purposes is distinct from other types of residence.
- ✦ Note that you may use a physical location that is not a valid mailing address. If you can describe the place where you stay so the municipal clerk can locate it on a map, any fixed location may be used as your "residence" for voting purposes. However, you may still have to provide a document for proof of residence, and any such document would have to identify that physical location. See below for proof of residence rules.
- ✦ All voters must provide a Proof of Residence document when registering… Acceptable proof of residence documents includes a letter on public or private social service agency letterhead identifying a homeless voter and describing the individual's residence for voting purpose.[4]

Contact local election officials well in advance of any voter registration deadline if you believe there may be doubt about your residency for voting purposes.[5]

[4] https://elections.wi.gov/resources/quick-reference-topics/enabling-qualified-homeless-individuals-vote.

[5] For a state-by-state summary of the relevant laws, see **Homeless and Low-Income Voter Rights Manual 2019,** https://nationalhomeless.org/wp-content/uploads/2019/07/2019-Manual-for-web.pdf.

AMERICAN OVERSIGHT



Voting Tip #11
Volunteer to Help Administer Elections

If you want to make certain elections are free and fair, help administer them. Apply to be a poll worker. (Yes, you get paid!)

There are all types of jobs available for every type of skill set. So don't be shy about applying. Do it NOW because you must be scheduled for training! If you'd like to be an elections worker in Pinellas County, Florida, for example, here's the basics:

What are the requirements to become a poll worker?

- You must be a registered or pre-registered voter in Pinellas County.
- All poll workers must be able to read and write English.
- You must attend the required poll worker training class or classes (based on poll worker position).

What are the poll worker positions?

- **Clerk:** Oversees all operations at the polling place, with added responsibilities prior to Election Day, such as contacting all the workers, picking up supplies, and setting up the voting equipment for the polling place. The Clerk communicates with the Election Call Center to verify voter eligibility; updates voter addresses; administers provisional ballots; assists in closing down the polling place; and is responsible for transmitting ballot totals after the polls close.
- **Assistant Clerk**: Assists the clerk in setting up the voting equipment; serves as a backup for all poll worker positions; communicates with the Elections Call Center to verify voter eligibility; makes sure that required forms are properly completed; assists in closing down the polling place; performs other duties specified by the Clerk.
- **Machine Manager**: Assists in setting up voting equipment before or on Election Day; handles the technical support requirements of the voting equipment; assists voters; and assists in closing down the polling place; is

~ Copyright by Sharon Lawrence 23 ~

AMERICAN OVERSIGHT

responsible for transporting the ballots to a designated site after the polls close.

- **Inspector:** Responsible for verifying voter eligibility; "check-in" voters using Electronic Voter Identification Device (EVID); provides voter with documentation so voter may obtain a ballot; and assists in closing down the polling place.
- **Precinct Deputy:** Maintains order at the polling place; ensures the polling place is ADA (i.e., Americans with Disabilities Act) compliant; designates the "no political activity" area outside the polling place; distributes voting supplies on Election Day; and assists in closing down the polling place.

Do I get paid for being a poll worker? Yes, after being selected to work in an election, poll workers are paid per class for their training. Pay varies from $150 to $265, depending on the assigned position.

What are the work hours on Election Day? All poll workers must be at their assigned polling place by 5:30 a.m., or earlier, on Election Day. Florida State Law requires polls to be open from 7:00 a.m. to 7:00 p.m. The day ends for poll workers when all votes have been accounted for and all materials have been packed away, usually around 8:00 p.m.

Poll workers are not permitted to leave their assigned polling places on Election Day. Poll workers must arrive with all the materials they will need for the entire day, such as food, drink, and medicine. Election Day is a long day; however, breaks and a lunch period are scheduled by the Clerk.

How do I vote if I do not work in my home precinct? Poll workers working outside of their home precinct will need to vote early or by mail prior to Election Day. Mail ballots must be returned to one of our three Elections Offices by 7:00 p.m. on Election Day.

What else should I know about serving as a poll worker?

- Poll workers are not guaranteed to work every election and may not necessarily work in their home precincts or with friends and family. Poll workers serve at the will of the Supervisor of Elections. Poll workers must be able to work as a team and must be courteous and helpful to voters.
- Poll worker assignments are based on experience, political party balance, and your availability to work. It is also important to know that the more conditions you place on your availability to work may reduce your placement options.
- If your preference is to work with a specific person, include the person's name on your online application in the comments section. We will make every reasonable attempt to place you in a polling location where you can work together.
- Some organizations donate their poll worker pay to charity. Please indicate the organization's name on your online application in the comments.

AMERICAN OVERSIGHT

- Poll workers must have their own transportation to class and to their assigned polling places on Election Day. Since Machine Managers will be transporting election materials and ballots after closing, they must have their own transportation on Election Day.
- Poll workers are not permitted to eat, drink, smoke, read the newspaper or use electronic devices while performing their duties as poll workers. These activities may be done on scheduled breaks outside the view of voters. Smoking is not allowed inside the polling place. Smoking breaks must be approved and scheduled with the precinct clerk.
- Poll workers are representatives of the Supervisor of Elections Office, which is a NONPARTISAN Office. It is strictly prohibited to provide information, advice or comments about candidates or issues while serving as a poll worker. Poll workers are not allowed to wear campaign buttons, T-shirts or any other item that may be considered political.
- Poll worker checks are mailed 3 to 4 weeks after each election.[6]

For more information about serving as a poll worker, call your local elections office or see https://www.nass.org/can-i-vote/become-a-poll-worker.

[6] https://www.votepinellas.com/Become-an-Election-Worker/Poll-Worker-Information#:

AMERICAN OVERSIGHT



Voting Tip #12
Develop a Firm Grasp of the Voter Identification Requirements, If Any

Obtain the Necessary Documentation If You Do Not Already Possess It

Be mindful of the requirements, if any, for identification (especially identification that includes your photograph) as you plan to vote as there are both federal and state laws that require some sort of (trustworthy) proof you are who you say you are.

~ Copyright by Sharon Lawrence 26 ~

AMERICAN OVERSIGHT

Federal Voter Identification Requirements. With the passage of the Help America Vote Act, individuals voting for the first time must present one of the designated forms of identification if they did not register in person.[7] To meet that requirement, registrants must:

- … provide their driver's license number or the last four digits of their social security number with their registration application.
- If the applicant has not been issued one of these numbers, the State must assign a unique identification number for voter registration purposes.
- Voters who have registered to vote by mail after January 1, 2003, who have not voted previously in a federal election in the state, and who do not fall within certain exceptions will be permitted to vote on a machine only after presenting one of the following items to election officials: current and valid photo identification, utility bill, bank statement, government check, paycheck, or government document that shows the voter's name and address. Copies of the required identification may be provided in advance of Election Day.[8]
- Military and overseas voters who vote by absentee/by mail ballot under the federal Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) are exempt from ALL voter ID requirements; and
- Elderly and disabled voters are exempt from federal first-time voter identification requirements but might not be exempt from state voter ID laws.[9]

State Voter Identification Requirements. The National Conference of State Legislatures reports that 35 states impose some sort of identification requirement on individuals seeking to vote. In addition to the District of Columbia and the territories, states without such a requirement are:[10]

- California
- Illinois
- Maine
- Maryland
- Massachusetts
- Minnesota
- Nebraska
- Nevada
- New Jersey
- New Mexico
- New York
- North Carolina
- Oregon
- Pennsylvania
- Vermont

---

7 https://www.eac.gov/about_the_eac/help_america_vote_act.aspx.

8 https://www.brennancenter.org/sites/default/files/analysis/HAVA%20Fact%20Sheet.pdf.

9 https://www.vote.org/voter-id-laws. (Includes state-by-state summary of voter identification laws).

10 https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx

AMERICAN OVERSIGHT

Ballot initiatives[11] and court challenges are constantly underway to voter identification requirements so voters must contact their local elections office for the current requirements in that jurisdiction.

[11] Nebraskans will vote on this issue during the General Election 2022.

~ Copyright by Sharon Lawrence 28 ~

AMERICAN OVERSIGHT



Learn About the Candidates & and the Issues on the Ballot

~ Copyright by Sharon Lawrence 29 ~

AMERICAN OVERSIGHT

Commonwealth of Virginia
Sample Ballot
County of Grayson
General Election
Tuesday, November 2, 2021

Instructions:

To vote for a candidate, use a black ballpoint pen to fill in the oval next to the name.
To vote for a candidate who is not on the ballot, fill in the oval next to the "Write-in" line and print that person's name clearly on the line.
If you want to change a vote or have made a mistake, ask an election official for another ballot. Do not make marks other than filling the oval.



Governor
Vote for only one
- Glenn A. Youngkin - R
- Terry R. McAuliffe - D
- Princess L. Blanding - LP
- _____ Write-in

Lieutenant Governor
Vote for only one
- Winsome E. Sears - R
- Hala S. Ayala - D
- _____ Write-in

Attorney General
Vote for only one
- Jason S. Miyares - R
- Mark R. Herring - D
- _____ Write-in

Member
House of Delegates
5th District
Vote for only one
- Israel D. O'Quinn - R
- Mathew N. Matsunaga - D
- _____ Write-in

Member
Board of Supervisors
Elk Creek District
Vote for only one
- Tracy A. "Zeke" Anderson
- Brenda R. Sutherland
- _____ Write-in

Member
School Board
Elk Creek District
Vote for only one
- Fred W. Weatherman
- _____ Write-in

Authorized by the Electoral Board of the County of Grayson
129 Davis St., Room 101 • Independence, VA, 24348
The authority statement printed above must be removed and replaced with the appropriate authority statement for the candidate, committee, individual or group using this ballot for their own purposes. The authority statement used for this ballot must comply with the requirements of either federal or state law, as appropriate. For state requirements, see §24.2-955 et seq. of the *Code of Virginia*. For federal requirements, call the Federal Election Commission, 1-800-424-9530.

Ballot Style # 002

Typ:01 Seq:0002 Spl:01

SAMPLE

Tip #13
To Know Which Races & Issues Will Be Before You, Look for a Sample Ballot

Your voter registration certificate will tell you to the Congressional, state legislative, and other districts to which you've been assigned. But how do you know when those races will be on the ballot, who the candidates will be, or what other issues might be put before the voters in a coming election?

AMERICAN OVERSIGHT

Elections officials cut through the stream of information coming at voters by preparing and sharing widely Sample Ballots for upcoming elections. Those will be posted online and may be printed in local news outlets, as well as distributed by interested organizations (e.g., political parties).

The form they take will differ among jurisdictions. As shown above, Grayson County, Virginia prints a mock ballot. As shown below, the Texas Secretary of State prepares a spreadsheet listing the candidates for statewide office.

No. 0000

GENERAL ELECTION (ELECCIÓN GENERAL)
(CONDADO DE) SAMPLE COUNTY, TEXAS
NOVEMBER 8, 2022 (8 DE NOVIEMBRE DE 2022)
SAMPLE BALLOT (BOLETA DE MUESTRA)

INSTRUCTION NOTE: Vote for the candidate of your choice in each race by placing an "X" or filling in the shape beside the candidate's name.
NOTA DE INSTRUCCIÓN: Vote por el candidato de su preferencia en cada carrera poniendo una "X" o rellenando la forma al lado del nombre del candidato.

Candidate for: (Candidato para:)	Republican Party (Partido Republicano)	Democratic Party (Partido Demócrata)	Libertarian Party (Partido Libertario)	Green Party (Partido Verde)	Independent (Independiente)
United States Representative, District _____ *(Representante de los Estados Unidos, Distrito Núm. _____)*					
Governor *(Gobernador)*	☐ Greg Abbott	☐ Beto O'Rourke	☐ Mark Tippetts	☐ Delilah Barrios	
Lieutenant Governor *(Gobernador Teniente)*	☐ Dan Patrick	☐ Mike Collier	☐ Shanna Steele		
Attorney General *(Procurador General)*	☐ Ken Paxton	☐ Rochelle Mercedes Garza	☐ Mark Ash		
Comptroller of Public Accounts *(Contralor de Cuentas Públicas)*	☐ Glenn Hegar	☐ Janet T. Dudding	☐ V. Alonzo Echevarria-Garza		
Commissioner of the General Land Office *(Comisionado de la Oficina General de Tierras)*	☐ Dawn Buckingham	☐ Jay Kleberg		☐ Alfred Molison, Jr.	
Commissioner of Agriculture (Comisionado de Agricultura)	☐ Sid Miller	☐ Susan Hays			
Railroad Commissioner *(Comisionado de Ferrocarriles)*	☐ Wayne Christian	☐ Luke Warford	☐ Jaime Andres Diez	☐ Hunter Wayne Crow	

Loudon County, Virginia takes yet another approach (see following page). Election officials post each "Ballot Style" (a given combination of races and issues matching a certain geographic area) and the list of precincts that will use that ballot style. Voters must check their voter registration certificates to see which precinct they have been assigned to, then match it to a ballot style.

Yet other jurisdictions have software online that allows voters to input their address to produce their customized sample ballot. **Note:** You may carry a marked Sample Ballot with you into the voting booth to help speed voting. You must, however, remove that list when you leave the voting booth.

AMERICAN OVERSIGHT

Sample Ballots

What's on the Ballot?

A sample ballot is a document that helps voters prepare for an election. It helps voters know what is on the ballot before they vote. Ballots look different for each

s and Elections Voters Candidates & Campaigns Get Involved About Us
egistration

e sure to look at your sample ballot before you vote.

November 8, 2022, General Election Sample Ballots

- Ballot Style 1 (PDF) - for voters in precincts 107, 108, 112, 114, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 207, 208, 209, 210, 213, 214, 215, 216, 217, 218, 219, 301, 302, 303, 305, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 318, 319, 320, 321, 322, 401, 402, 403, 407, 408, 409, 411, 413, 414, 416, 420, 421, 422, 701, 702, 703, 705, 707, 708, 709, 710, 808, 810, 813, 814, 815, 817, 818, 819, 820, 822
- Ballot Style 3 (PDF) - for voters in the Town of Purcellville precincts 301 and 310 (non-town voters use ballot style 1)
- Ballot Style 4 (PDF) - for voters in the Town of Round Hill precinct 302 (non-town voters use ballot style 1)
- Ballot Style 5 (PDF) - for voters in the Town of Hillsboro precinct 303 (non-town voters use ballot style 1)
- Ballot Style 6 (PDF) - for voters in the Town of Lovettsville precinct 401 (non-town voters use ballot style 1)
- Ballot Style 7 (PDF) - for voters in the Town of Leesburg precinct 408 (non-town voters use ballot style 1)
- Ballot Style 8 (PDF) - for voters in the Town of Hamilton precinct 416 (non-town voters use ballot style 1)
- Ballot Style 9 (PDF) - for voters in the Leesburg School Board District precincts 501, 502, 503, 504, 505, 506, 507, 508, 509, 510 (town voters use ballot style 10)
- Ballot Style 10 (PDF) - for voters in the Town of Leesburg precincts 501, 502, 503, 504, 505, 506, 507, 508, 509, 510 (non-town voters use ballot style 9)
- Ballot Style 11 (PDF) - for voters in the Broad Run School Board District precincts 615, 616, 617, 619, 620, 621, 622, 623, 625, 626, 627, 628, 629
- Ballot Style 2 (PDF) - Federal Only Ballot - only for registered voters who are citizens of the United States who have indicated that they currently reside overseas with no intention of returning soon

Voters are encouraged to double-check their voting precinct at www.vote.virginia.gov to ensure they know their precinct number when viewing ballots.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 32 ~



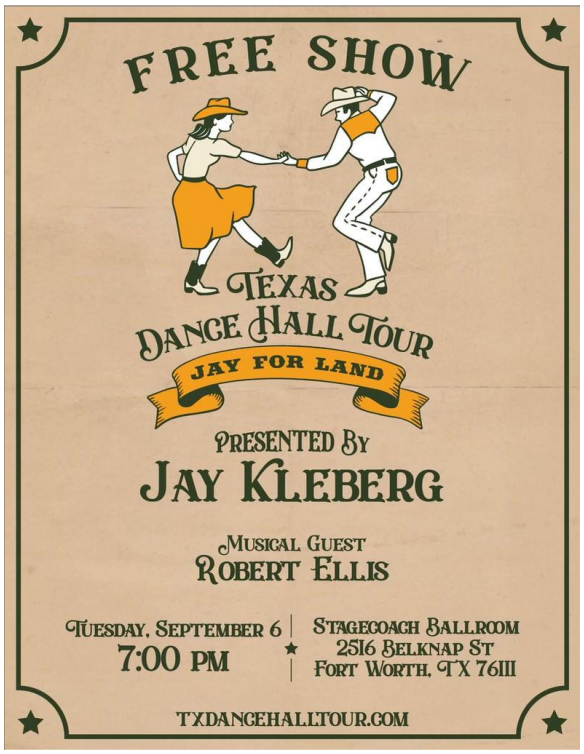
A sample of a candidate's Facebook page

~~~~~~~~~~~~

Voting Tip #14
Learn About the Candidates (from the Candidates)

Of course, each candidate will be utilizing a wide range of tools to communicate with voters, including:

- ✦ Advertisements on billboards, radio, signs, social media, television, and vehicles and in newspapers;
- ✦ Direct mail, email, or text messages to voters;
- ✦ Door to door campaigning (either by the candidate or by volunteers for him/her);
- ✦ Media interviews (e.g., podcasts, radio, and television);
- ✦ Personal appearances for the general public (e.g., Jay Kleberg's Texas Dance Hall Tour) and/or special interest groups (e.g., League of Women Voters sponsors candidate forums in many communities);
- ✦ Social Media (e.g., Facebook, Instagram, and Twitter); and
- ✦ Videos (see YouTube.com).

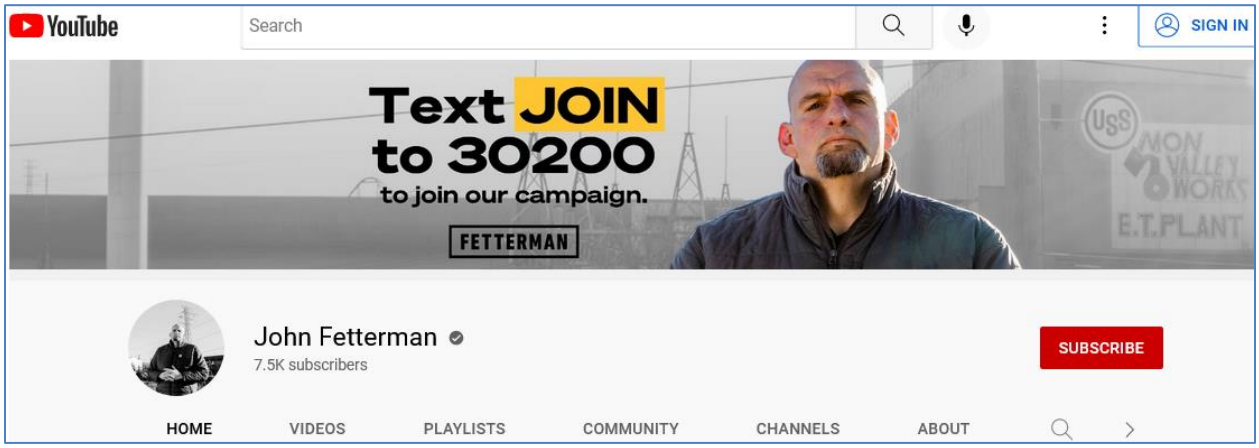


~ Copyright by Sharon Lawrence 33 ~

AMERICAN OVERSIGHT
~~~~~~~~~~~~



Many candidates (even those for local office) now are livestreaming their events (e.g., on Facebook) and archiving the tapings of those events for future viewing. See illustration below of YouTube's role in modern campaign communications.



~ Copyright by Sharon Lawrence 34 ~

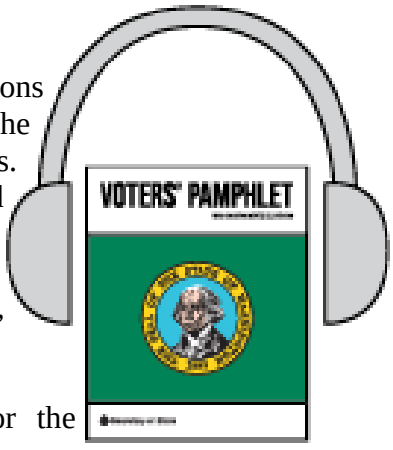
AMERICAN OVERSIGHT



Voting Tip #15
Learn About the Candidates (from Other Sources)

Voters have an almost unlimited sources of information about candidates to help them determine how to vote. For impartial, nonpartisan information on all the federal and state candidates and issues on your ballot, consult:

- ✦ League of Women Voters, whose 50 state and more than 700 local chapters sponsor town hall meetings with candidates and produce voters guides covering federal, state, and most local election; https://www.lwv.org/about-us/membership-local-leagues;
- ✦ PolitiFact, which investigates the veracity of the statements of elected officials and candidates, https://www.politifact.com; and
- ✦ Vote Smart for information on federal and state candidates and ballot issues, https://justfacts.votesmart.org/about/.

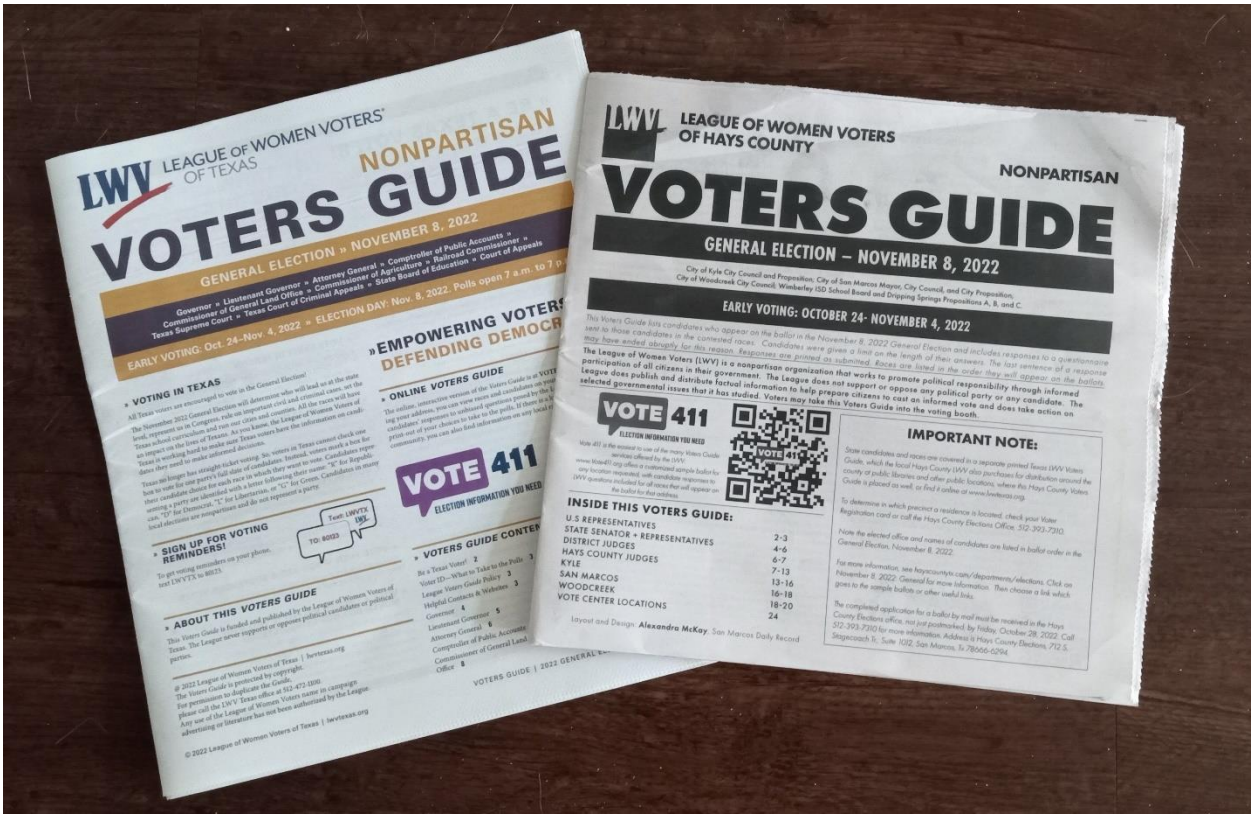


Official Voter Guides. In a number of states, the Chief Elections Official is required by law to prepare a non-partisan guide about the upcoming election for automatic distribution to all registered voters. That guide includes statements from the candidates and supporters/opponents of ballot issues plus other materials.

Washington State produces its voter guide in multiple formats, presenting the information in:

- ✦ A dynamic, searchable, online guide (customizable for the individual voter);

AMERICAN OVERSIGHT





✦ Print, either as a PDF document or a flat/plain text file;
✦ Audio MP3 format; and
✦ Video.

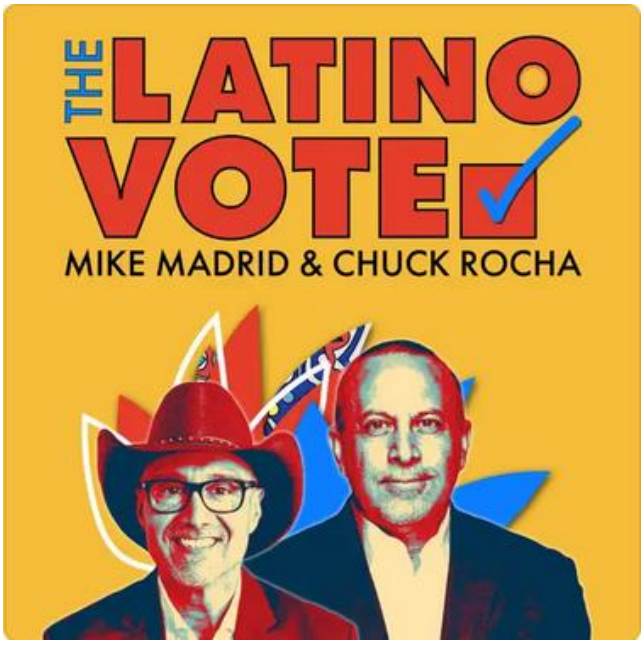
For the 2020 presidential election, the state produced 31 editions of the print guide, including versions in Chinese, Spanish, and Vietnamese.

Other Sources of Information. Along with their standard coverage of the campaign, newspapers also publish detailed guides for their readers covering not only the candidates and ballot issues, but also sharing voting information (e.g., location of polling places).

In addition to exploring the coverage provided by local and national for-

AMERICAN OVERSIGHT
~ Copyright by Sharon Lawrence 36 ~





profit newspapers, voters should consult non-profit news services (such as Atlanta's **Capitol Beat** and the **Texas Tribune**).

Radio and television stations may produce voter guides in conjunction with their programming, which, for many, includes hosting live candidate debates.

Non-profit organizations also have taken on the responsibility of voter education. Examples include the **Progressive Voter Guide** produced by Courage California[12] and the **Georgia Voter Guide.**[13]

Advocacy groups (such as the Animal Welfare Institute) also will be sharing their insights into the candidates' positions as may local business organizations (e.g., Chambers of Commerce).

Podcasts, Radio/Television Interviews, and Town Halls. Voters eager to learn more about candidates or issues on the ballot, especially at the national level, have plenty of audio and video options available to them. Past broadcasts of C-SPAN and National Public Radio (NPR) are readily available after their initial airing.

Similarly, podcasts[14] featuring political discussions from all across the spectrum for federal, state, and local government politics may be at your fingertips.[15] The Yonder Report, for example, focuses on rural issues.

---

12 https://progressivevotersguide.com/california.

13 https://www.georgiavoter.guide.

14 Defined as a "digital audio file made available on the internet for downloading to a computer or mobile device, typically available as a series, new installments of which can be received by subscribers automatically."

15 https://www.weeditpodcasts.com/21-of-the-best-podcast-directories-of-2021/.

AMERICAN OVERSIGHT



Tip #16
Don't Forget to Educate Yourself on the Judges/Justices Seeking Election or Retention

States vary widely in the way they handle selection to and retention of judges to the various state and local courts. Options for state courts include:

- ✦ Appointed by governor, lifetime appointment;
- ✦ Appointed by the state legislature, lifetime appointment;
- ✦ Appointed by governor, subject to a periodic retention vote;[16]
- ✦ Elected by the public on a non-partisan basis; and
- ✦ Elected by the public on a partisan.

Thirty-eight (38) states have some form of election for state Supreme Court justices. Election practices differ with some states selecting the candidates through party primaries. Others utilize the "jungle primary" approach whereby all candidates run in one primary with the top vote getters advancing to the General Election regardless of party affiliation.

[16] In a retention vote, at given intervals (e.g., every ten years) a judge's name is placed on the ballot and the electorate is asked, "Should Judge/Justice [insert name] be retained in office?" Those who receive the given level of affirmative votes (e.g., 60 percent) continue on the bench for the given interval.

AMERICAN OVERSIGHT



Voting Tip #17
Study the Issues That Will Appear on the Ballot

Voters don't make their preferences known just on candidates for office. They also may be asked to take a stand on a public expenditure (e.g., approve the issuance of bonds to finance the construction of a new high school) or a policy issue (e.g., removal of the criminal penalties for use of cannabis) at election time. These issues come onto the ballot in one of two ways.

- Citizens circulate petitions asking that an issue be placed before the voters (i.e., initiative), or
- State or local legislators take official action to put an issue on the ballot (i.e., referendum process).

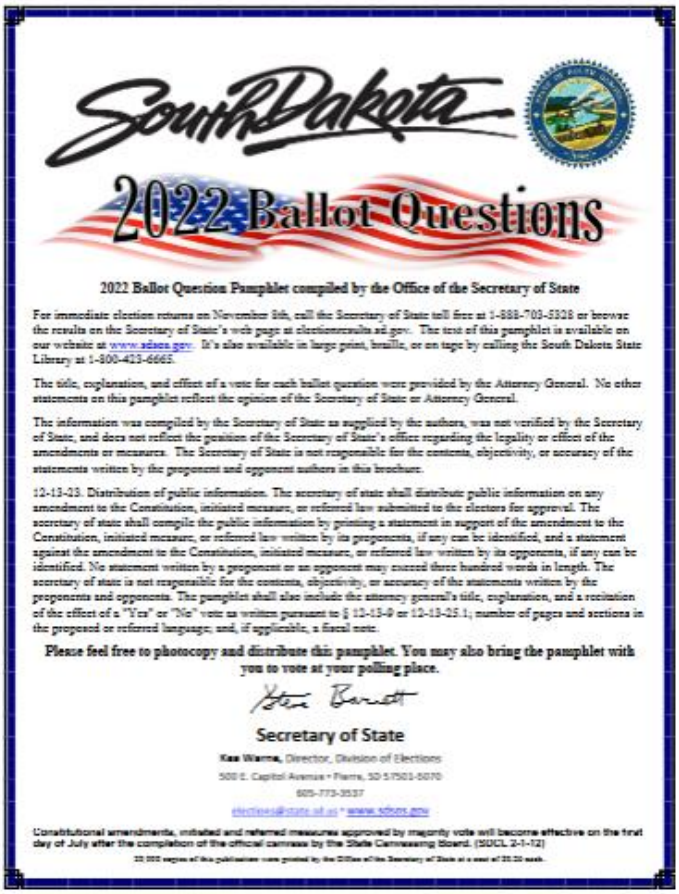
State laws vary substantially, however, on the authorization for initiative and referendum,[17] As of this writing, initiative and/or referendum law are in force in the following states and territories:

- Alaska
- Arizona
- Arkansas
- California

[17] https://ballotpedia.org/States_with_initiative_or_referendum.
https://www.ncsl.org/research/elections-and-campaigns/chart-of-the-initiative-states.aspx.

AMERICAN OVERSIGHT

- ✦ Colorado
- ✦ Florida
- ✦ Idaho
- ✦ Illinois
- ✦ Maine
- ✦ Maryland
- ✦ Massachusetts
- ✦ Michigan
- ✦ Mississippi
- ✦ Missouri
- ✦ Montana
- ✦ Nebraska
- ✦ Nevada
- ✦ New Mexico
- ✦ North Dakota
- ✦ Ohio
- ✦ Oklahoma
- ✦ Oregon
- ✦ South Dakota
- ✦ Utah
- ✦ Washington
- ✦ Wyoming
- ✦ District of Columbia
- ✦ US Virgin Islands



South Dakota

2022 Ballot Questions

2022 Ballot Question Pamphlet compiled by the Office of the Secretary of State

For immediate election returns on November 8th, call the Secretary of State toll free at 1-888-703-5328 or browse the results on the Secretary of State's web page at electionresults.sd.gov. The text of this pamphlet is available on our website at www.sdsos.gov. It's also available in large print, braille, or on tape by calling the South Dakota State Library at 1-800-423-6665.

The title, explanation, and effect of a vote for each ballot question were provided by the Attorney General. No other statements on this pamphlet reflect the opinion of the Secretary of State or Attorney General.

The information was compiled by the Secretary of State as supplied by the authors, was not verified by the Secretary of State, and does not reflect the position of the Secretary of State's office regarding the legality or effect of the amendments or measures. The Secretary of State is not responsible for the contents, objectivity, or accuracy of the statements written by the proponent and opponent authors in this brochure.

12-13-23. Distribution of public information. The secretary of state shall distribute public information on any amendment to the Constitution, initiated measure, or referred law submitted to the electors for approval. The secretary of state shall compile the public information by printing a statement in support of the amendment to the Constitution, initiated measure, or referred law written by its proponents, if any can be identified, and a statement against the amendment to the Constitution, initiated measure, or referred law written by its opponents, if any can be identified. No statement written by a proponent or an opponent may exceed three hundred words in length. The secretary of state is not responsible for the contents, objectivity, or accuracy of the statements written by the proponents and opponents. The pamphlet shall also include the attorney general's title, explanation, and a recitation of the effect of a "Yes" or "No" vote as written pursuant to § 12-13-9 or 12-13-25.1; number of pages and sections in the proposed or referred language; and, if applicable, a fiscal note.

Please feel free to photocopy and distribute this pamphlet. You may also bring the pamphlet with you to vote at your polling place.

Secretary of State

Kea Warne, Director, Division of Elections

500 E. Capitol Avenue • Pierre, SD 57501-5070

605-773-3537

electionsd@state.sd.us • www.sdsos.gov

Constitutional amendments, initiated and referred measures approved by majority vote will become effective on the first day of July after the completion of the official canvass by the State Canvassing Board. (SDCL 2-1-12)

Fortunately for voters, several sources track the measures as they are approved for a public vote:

- ✦ Ballotpedia[18] and
- ✦ National Conference of State Legislatures.[19]

In addition to voting on policy issues, voters should be alert to ballot items that ask them to approve/disapprove the issuance of bonds by state or local government entities to finance non-recurring expenditures (e.g., building a new school). As of this writing, there's no national tracking system for those state and local government measures but they will be listed on all sample ballots and included in most/all voter guides.

For impartial information about the measure, look for official government publications such as the above one produced by the South Dakota Secretary of State's office in accordance with state law. Nebraska law requires not only the preparation of a voter information pamphlet, it also mandates the conduct of at least one public hearing in each Congressional district on proposed ballot measures.[20]

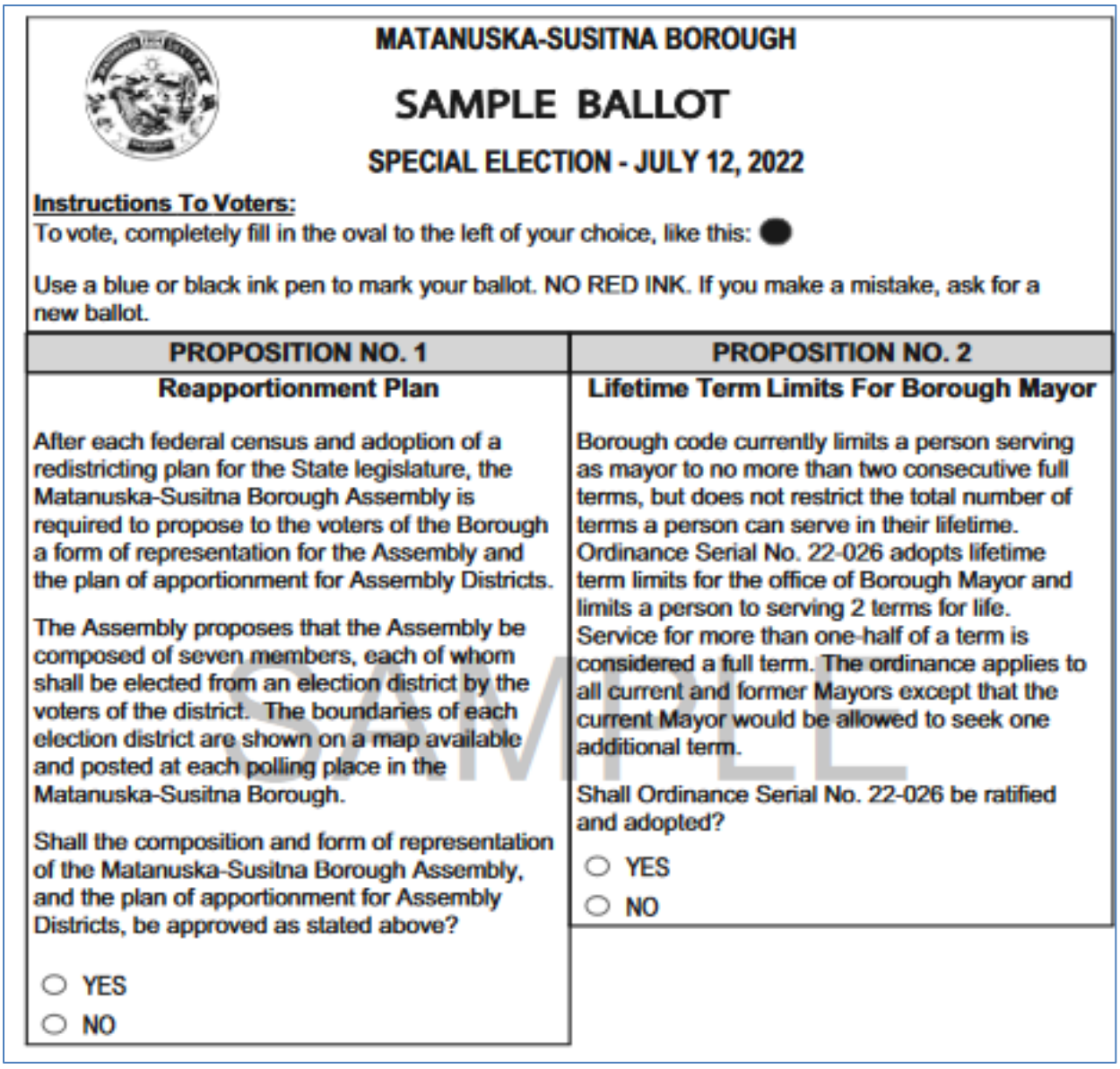
---

18 https://ballotpedia.org/2022_ballot_measures.

19 https://www.ncsl.org/research/elections-and-campaigns/ballot-measures-database.aspx.

20 https://azsos.gov/elections/ballot-measures/2022-ballot-measure-information.
Arizona law also requires town hall meetings on statewide ballot propositions.

AMERICAN OVERSIGHT



MATANUSKA-SUSITNA BOROUGH

SAMPLE BALLOT

SPECIAL ELECTION - JULY 12, 2022

Instructions To Voters:
To vote, completely fill in the oval to the left of your choice, like this: ●

Use a blue or black ink pen to mark your ballot. NO RED INK. If you make a mistake, ask for a new ballot.

PROPOSITION NO. 1
Reapportionment Plan

After each federal census and adoption of a redistricting plan for the State legislature, the Matanuska-Susitna Borough Assembly is required to propose to the voters of the Borough a form of representation for the Assembly and the plan of apportionment for Assembly Districts.

The Assembly proposes that the Assembly be composed of seven members, each of whom shall be elected from an election district by the voters of the district. The boundaries of each election district are shown on a map available and posted at each polling place in the Matanuska-Susitna Borough.

Shall the composition and form of representation of the Matanuska-Susitna Borough Assembly, and the plan of apportionment for Assembly Districts, be approved as stated above?

○ YES
○ NO

PROPOSITION NO. 2
Lifetime Term Limits For Borough Mayor

Borough code currently limits a person serving as mayor to no more than two consecutive full terms, but does not restrict the total number of terms a person can serve in their lifetime. Ordinance Serial No. 22-026 adopts lifetime term limits for the office of Borough Mayor and limits a person to serving 2 terms for life. Service for more than one-half of a term is considered a full term. The ordinance applies to all current and former Mayors except that the current Mayor would be allowed to seek one additional term.

Shall Ordinance Serial No. 22-026 be ratified and adopted?

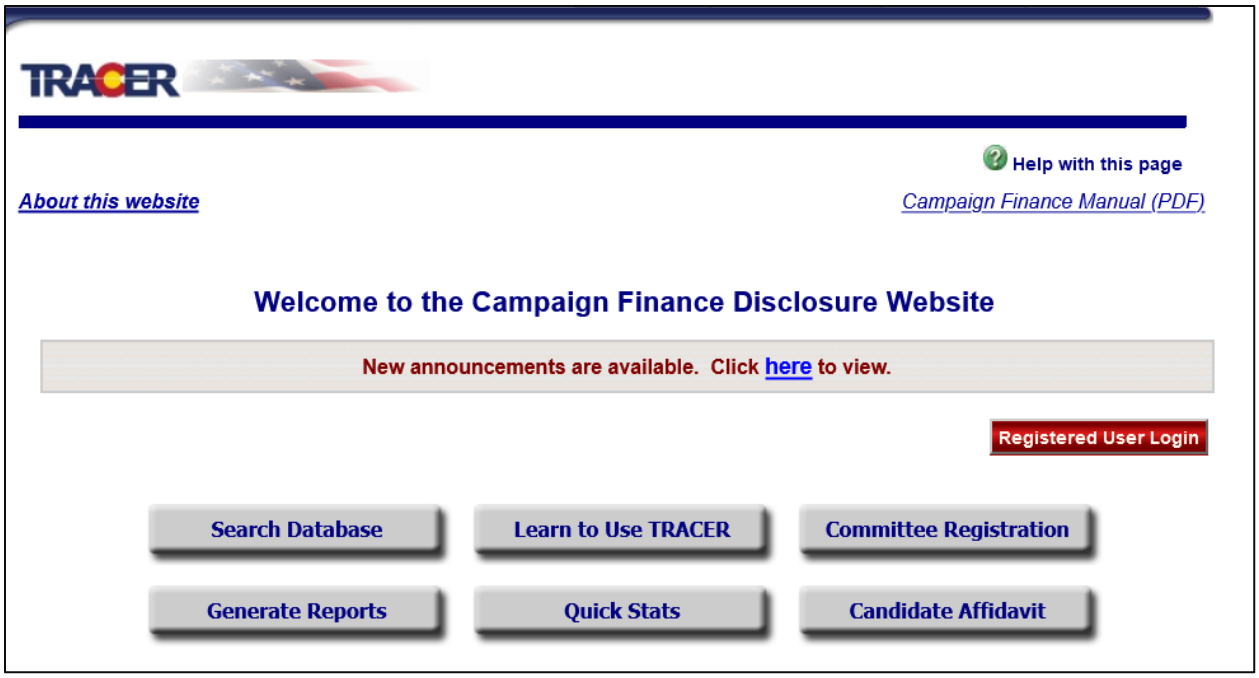
○ YES
○ NO

SAMPLE

Sample of a ballot for an issue, not an office

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 41 ~



Tracer, Colorado's Campaign Finance Disclosure Website

~~~~~~~~

Voting Tip #18
Know Who is Financing the Campaigns

As you begin to study candidates closely, data that may be of substantial interest to you may be the sources of a candidate's campaign funds.

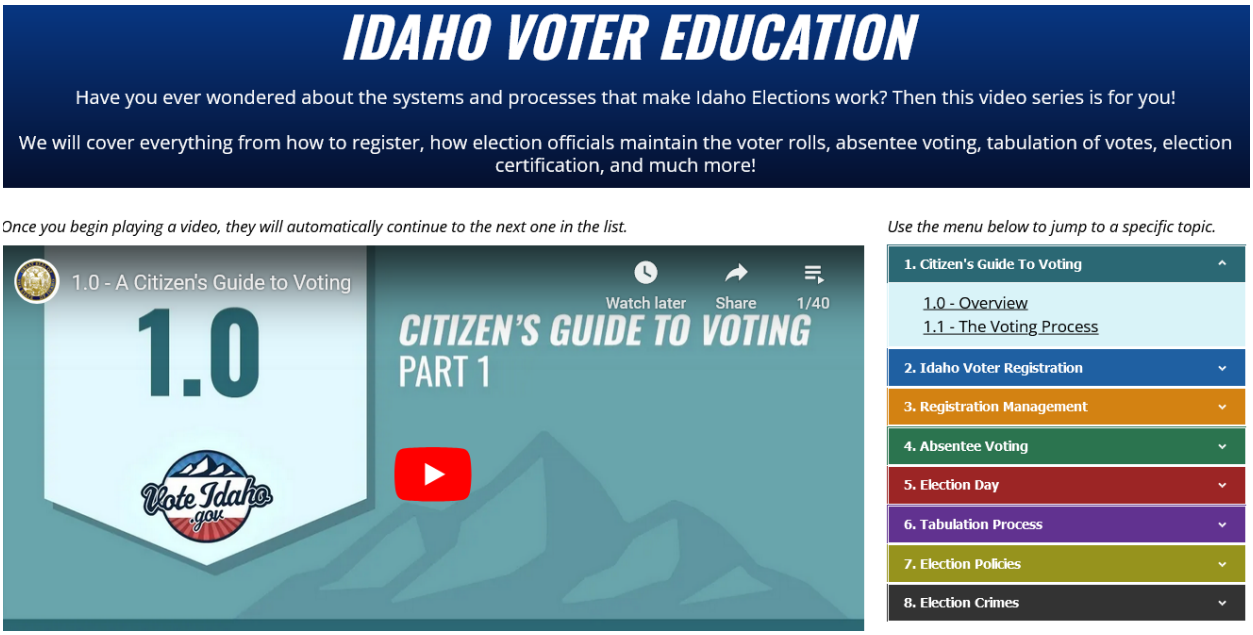
Government Agencies. For detailed information in that point for all federal candidates, consult the website for the Federal Election Commission (FEC), https://www.fec.gov/data.

Curious as to who is funding the campaigns of candidates for state office? Ballotpedia has made research in this regard easy for you, with the following links to all state campaign finance agencies, https://ballotpedia.org/State_campaign_finance_agencies.

Non-Profit Entities. Among the non-governmental sources tracking campaign spending at the federal and state level, for both candidates and ballot measures, OpenSecrets is at the top of the list, https://www.opensecrets.org.

~ Copyright by Sharon Lawrence 42 ~

AMERICAN OVERSIGHT
~~~~~~~~

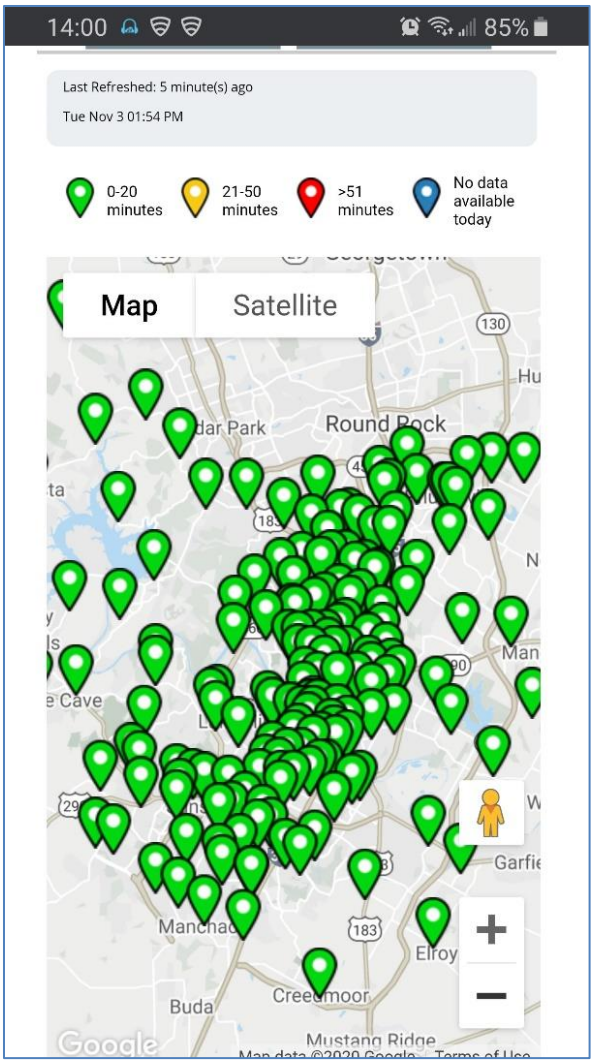


Understand the Voting Process

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 43 ~

Tip #19
Determine When and Where You May Vote In-Person



For many people, voting on Election Day means a trip to an assigned polling place in their neighborhood. To determine where you should go on Election Day, look at your voter registration certificate. It will list the precinct to which you have been assigned. Addresses for the polling place serving that precinct will be published in the local newspaper on/before Election Day and on the election office website. You may telephone the elections office as well for that information.

With the advent of Early Voting[21] and Vote Centers,[22] many people have options about when and where they may vote in-person. Check the calendar for your community and pick a day and place for this important task. Days and hours that the polls are open will vary during Early Voting periods.

Some jurisdictions are enhancing decision-making by providing real-time mapping of the estimated wait times at each polling location. (See illustration above from Travis County, Texas.)

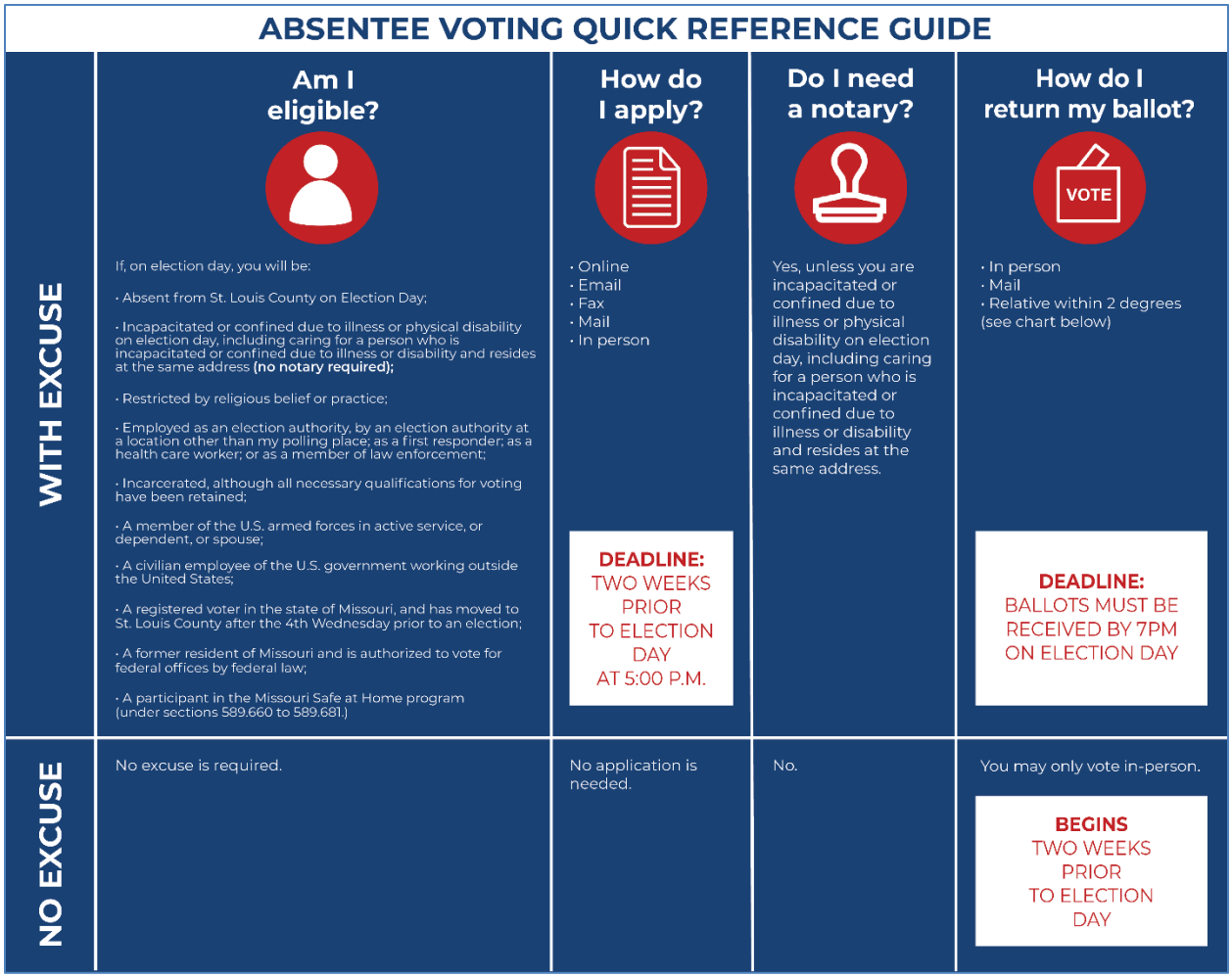
---

[21] A multi-day period for in-person voting prior to the official Election Day (e.g., October 24 – November 4, 2022 prior to Election Day on November 8, 2022).

[22] A central location where any voter registered in the county may cast his/her ballot.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 44 ~



Absentee Voting Instructions for St. Louis, Missouri[23]

~~~~~~~~~~

Tip #20
Determine If You May Vote Absentee /By Mail Instead

Many voters may prefer to vote by mail rather than in-person, either for convenience or of necessity. The options to do so vary widely by state. Several states now have "no excuse" absentee voting (i.e., no reason required).[24] Among that states that still require that a voter meet certain criteria to vote Absentee/By Mail, South Carolina extends that option to persons:

23 https://stlouiscountymo.gov/st-louis-county-government/board-of-elections/elections/absentee-voting/.

24 Michigan and Wisconsin.

AMERICAN OVERSIGHT
~~~~~~~~~~

- With employment obligations which prevent them from voting during early voting hours for the duration of the early voting period, and during the hours the polls are open on Election Day.
- Attending a sick or physically disabled person which prevents them from voting during early voting hours for the duration of the early voting period, and during the hours the polls are open on Election Day.
- Confined to a jail or pretrial facility pending disposition of arrest or trial which prevents them from voting during early voting hours for the duration of the early voting period, and during the hours the polls are open on Election Day.
- Who will be absent from their county of residence during early voting hours for the duration of the early voting period, and during the hours the polls are open on Election Day.
- With physical disabilities.
- Sixty-five years of age or older.
- Who are members of the Armed Forces and Merchant Marines of the United States, their spouses, and dependents residing with them
- Admitted to a hospital as an emergency patient on the day of the election or within a four-day period before the election.[25]

Tennessee voters may request an Absentee/By Mail ballot under the following conditions:

- You are sixty (60) years of age or older.
- You will be outside the county where you are registered during the early voting period and all day on Election Day.
- You are hospitalized, ill or physically disabled and unable to appear at your polling place to vote (this includes persons who have underlying medical or health conditions which in their determination render them more susceptible to contracting COVID-19 or at greater risk should they contract it). A physician's statement is not required to check this box.
- You are the caretaker of a person who is hospitalized, ill, or disabled (this includes voters who care for or reside with persons who have underlying medical or health conditions which in their determination render them more susceptible to contracting COVID-19 or at greater risk should they contract it). A physician's statement is not required to check this box.
- You or your spouse are a full-time student in an accredited college or university outside the county where you are registered.
- You reside in a nursing home, assisted living facility or home for the aged outside your county of residence.
- You are a candidate for office in the election.
- You are observing a religious holiday that prevents you from voting in person during the early voting period and on Election Day.
- You serve as an Election Day official or as a member or employee of the election commission.
- You will be unable to vote in-person due to jury duty.

[25] https://scvotes.gov/voters/absentee-voting.

AMERICAN OVERSIGHT

- ✦ You have a physical disability and (are assigned to) an inaccessible polling place.
- ✦ You or your spouse possess a valid commercial driver's license (CDL), or Transportation Worker Identification Credential (TWIC) card and you will be working outside the state or county of registration during the open hours of early voting and Election Day and have no specific out-of-county or out-of-state address to which mail may be sent or received during such time.
- ✦ You are a member of the military or are an overseas citizen.
- ✦ You are on the permanent absentee list.[26]

Texas adds one unusual exception to its list, i.e., pregnant women nearing their due date: Authorized excuses for Absentee/By Mail voting in the Lone Star state are for the voter to be:

- ✦ 65 years or older;
- ✦ Sick or disabled;
- ✦ Out of the county on Election Day and during the period for early voting by personal appearance; or
- ✦ Expected to give birth within three weeks before or after Election Day; or
- ✦ Confined in jail, but otherwise eligible.[27]

[26] https://sos.tn.gov/elections/guides/guide-to-absentee-voting.
[27] https://www.sos.texas.gov/elections/voter/reqabbm.shtml.

AMERICAN OVERSIGHT



The physician above participates in the Vot-ER program to help hospitalized individuals exercise their right to vote.[28]

~~~~~~~~~~~

Tip #21
Voting in Case of a Family or Medical Emergency

Unforeseen emergencies may arise after the deadline for an absentee/by mail ballot which affect your ability to get to the polls on Election Day. That does NOT mean, however, that you lose the opportunity to cast a ballot.

Most states have established procedures to follow for emergency voting. The advocacy group Patient Voting identified 38 states with laws or regulations in place governing voting in case of a medical emergency.[29] Ohio law, for example, declares:

> If you or your minor child is in the hospital on Election Day, you must submit a properly completed and signed request to the board of elections of the county in which your voting residence is located by 3 p.m. on Election Day.
>
> To be eligible under this provision, you or your minor child must be confined in a hospital because of an accident or unforeseeable medical emergency. If you or your

[28] https://vot-er.org/
[29] https://www.patientvoting.com/howtovote.

AMERICAN OVERSIGHT
~~~~~~~~~~~

> minor child is hospitalized in the same county where you are registered to vote, two representatives of the board of elections can deliver the ballot to you, wait while you mark the ballot, and return your voted ballot to the board office.
>
> Additionally, you may include in your absentee/by mail ballot application a request that your county board of elections give your unmarked ballot to a designated relative – your spouse, father, mother, father-in-law, mother-in-law, grandfather, grandmother, brother, sister, son, daughter, adopted parent, adopted child, stepparent, stepchild, uncle, aunt, nephew or niece – who shall deliver the ballot to you in the hospital and return your voted ballot to the board office.[30]

Voters in Milwaukee, Wisconsin would take these steps to cast a ballot if hospitalized or quarantined:

> These voters need to appoint an agent to retrieve and deliver their absentee/by mail ballot if they are hospitalized in the 7 days before Election Day or on Election Day.
>
> 1. The voter can use MyVote.wi.gov to complete their absentee/by mail ballot request form or they can print and complete the form... In box 7 of the form, the voter has certified that they are hospitalized.
> 2. The voter then appoints an agent to request/deliver the ballot on the voter's behalf. The voter may appoint anyone as their agent. The agent will need to provide their information on the absentee/by mail ballot application. The agent's information should appear in box 7 of the form.
> 3. If the voter is not registered, the elector must complete a voter registration application…. The agent may deliver the registration along with the absentee/by mail ballot request. The voter will also need to provide a proof of residence document with their registration. A proof of residence document proves where the voter lives in Wisconsin.
> 4. The agent for the hospitalized voter delivers a completed absentee/by mail ballot application (and possibly the voter registration form) to the Election Commission office for the hospitalized or quarantined voter. The agent can deliver the form beginning 7 days before Election Day.
> 5. The agent must also show a copy of the voter's photo ID, or the voter's original photo ID, to the Election Commission when making the absentee/by mail ballot request…. An agent must provide his or her proof of identification before the municipal clerk may issue an absentee/by mail ballot to the agent.
> 6. The Election Commission issues an absentee/by mail ballot, absentee certificate envelope and uniform instructions in an absentee carrier envelope to the agent for the hospitalized or quarantined voter.
> 7. The agent transports the absentee/by mail ballot to the hospitalized or quarantined voter. The voter votes the ballot in the presence of a witness. The voter places the voted ballot in the absentee certificate envelope, seals and signs the envelope. The witness also needs to sign the absentee certificate envelope. The agent may serve as their witness.

30` https://www.ohiosos.gov/elections/voters/absentee-voting.

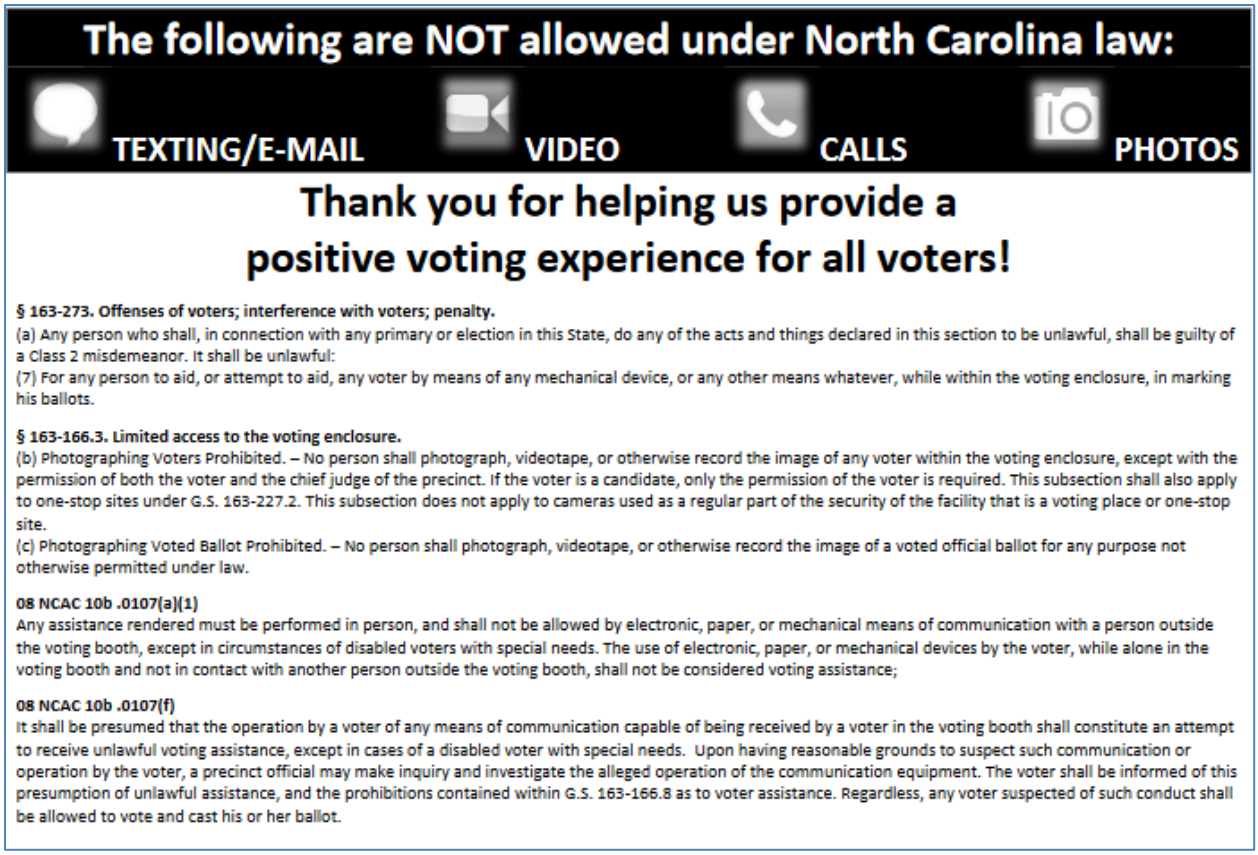
AMERICAN OVERSIGHT

8. The agent must deliver, mail or use a drop box to return the absentee/by mail ballot to the Election Commission. Whether the agent personally delivers the ballot, uses a drop box or mails the ballot, it must be received by the Election Commission by 7:30 p.m. on Election Day so that the ballot may be delivered to Central Count to be counted.[31]

Individuals who are ill but not hospitalized have the option of curbside voting in all jurisdictions. (See Tip # 33 for a description of that option).

[31] https://city.milwaukee.gov/election/Voter-Info/HospitalizedVoters.

AMERICAN OVERSIGHT



Tip #22
Be Mindful of What You May or May NOT Do At the Polling Place Or Near a Ballot Drop Box

Each state sets forth guidelines as to what is or is not acceptable conduct at the polling place or near a ballot drop box in order to protect the rights of voters to an orderly voting process free of coercion or intimidation. Common restrictions within a buffer zone surrounding a polling place (set by states at distances from 50 – 200 feet) address:

- Actions designed to influence voters or solicit votes,
- Advertising or peddling any product or service,
- Circulating petitions or soliciting signatures for petitions,
- Carrying or displaying campaign literature or signs,
- Conducting exit or public opinion polls,
- Loitering,
- Obstructing the entrance to a polling place or hindering voters in any way entering/inside/leaving the polling place,
- Projecting sounds referring to candidates or issues on the ballot, and

AMERICAN OVERSIGHT
~ Copyright by Sharon Lawrence 51 ~

- ✦ Wearing campaign apparel, buttons, or stickers (except for the "I Voted" sticker).[32]

Drawing upon Florida law, Brevard County, Florida advises voters of the following restrictions on polling place activities:

> **Persons Allowed in Polling Place and Early Voting Sites.** The list of persons permitted in the polling place and early voting areas is defined in Section 102.031, Florida Statutes, as:
>
> - ✦ Persons there to vote,
> - ✦ The Supervisor of Elections and/or his or her deputy,
> - ✦ Election clerks and inspectors,
> - ✦ Official poll watchers,
> - ✦ Persons in the care of a voter,
> - ✦ Persons caring for a voter,
> - ✦ Law enforcement officers and/or emergency service personnel (with the permission of the Clerk or a majority of the inspectors), and
> - ✦ Persons assisting with or participating in simulated elections for minors.
>
> Election boards have the full authority to maintain reasonable control and decorum at the polls including directing or removing persons within the polling room who otherwise are disrupting the electoral process.
>
> **Solicitation Area.** No person, political committee, or other group or organization may solicit voters inside the polling place or early voting site or within 150 feet of the entrance to any polling place, an early voting site, or an office of the Supervisor of Elections where vote-by-mail ballots are requested and printed on demand for the convenience of electors who appear in person to request them. Before the opening of the polling place or early voting site, the Clerk or Supervisor shall designate the no-solicitation zone and mark the boundaries.
>
> **Poll Watchers.** Poll watchers are approved initially by the Supervisor of Elections and are subject to the reasonable control of local election boards as are other individuals within the polling room or early voting site…. Poll watchers shall pose any questions regarding the polling place procedures directly to the Clerk for resolution. They may not interact with voters.
>
> **Prohibited Campaign Material.** Prohibited political advertisements or campaign paraphernalia for both poll workers and poll watchers include the following: clothing, buttons, hats, wristbands, badges and other similar items that promote the

[32] For a detailed state-by-state summary of laws on electioneering, see the National Conference of State Legislatures "Electioneering Prohibitions," https://www.ncsl.org/research/elections-and-campaigns/electioneering.aspx.

AMERICAN OVERSIGHT

election or defeat of a candidate or issue or engages in campaign sloganeering associated with any party, candidate or issue.

For example, any letter (e.g., "W"), phrase (e.g., "Every Voter Counts" or "Flip-Flop"), or any other indications that is or has become directly or indirectly associated with a political party, candidate, or group. Wearing of campaign or political advertisements by electors is not a violation unless the wearer makes overtures at the polling place/early voting site in advocacy of a particular candidate or his/her views regarding an issue on the ballot.

Items Permitted and Disallowed for Electors. Electors may take papers or other aids into the voting booth to refresh their memory and assist in expediting the voting process provided such use does not appear to be part of a concerted effort by an individual or group to subvert the normal election process. According to Section 104.19(1)(a), Florida Statutes, it is unlawful for any person casting a ballot to use stickers or rubber stamps or to carry into a voting booth any mechanical device, paper or memorandum which might be used to affect adversely the normal voting process. Violation is punishable as a second-degree misdemeanor.[33]

Protections against interfering with the elections process are now being extended to ballot drop boxes. Washington statutes state that no one may electioneer, circulate campaign materials, solicit petition signatures, or impede the voting process within twenty-five feet of a ballot deposit site that is not located within a voting center.[34]

See the Appendix for the detailed guidance offered by the Arizona Secretary of State for polling place conduct and the prevention of voter intimidation.

Selfies? At the Polling Place? At Home?

Of course, the question that comes to mind for many people is "What about selfies?" As noticed above, North Carolina law prohibits ballot selfies. But not all states follow suit. The Minnesota Secretary of State explains that state's approach to the matter, saying:

> There is no law that strictly prohibits taking photos or videos in the polling place to record your own voting experience. However, the Office of the Minnesota Secretary of State discourages this activity for the following reasons:
>
> > Voters have a right to privacy, both as to how an individual has voted as well as whether or not an individual has voted. Either or both of these could be compromised by pictures or video. In addition, other voters' objections to being photographed could lead to disruptions within the polling place.

[33] https://www.votebrevard.gov/Election-Information/Polling-Place-and-Early-Voting-Site-Regularions.
[34] Section 434-250-100(6).

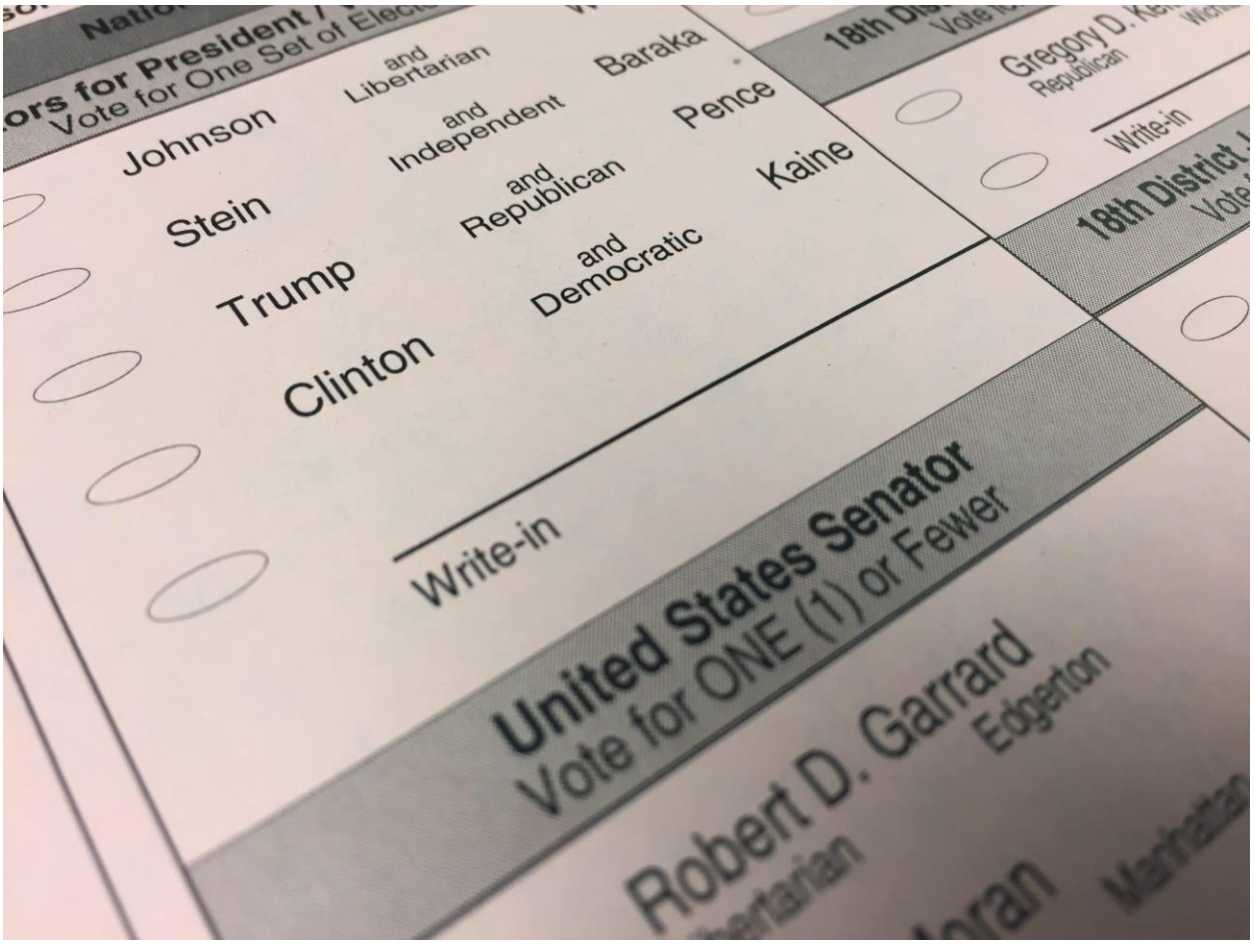
AMERICAN OVERSIGHT

When voter turnout is high there may be lines and polling places may be crowded. Voters have a right to take the time they need to vote but should not take extra time to take pictures.

In addition, Minnesota Statutes 204C.17 and Minnesota Statutes 204C.18 prohibit voters from showing their marked ballot to others. Taking photographs or video of your own marked ballot could violate this prohibition.[35]

[35] https://www.sos.state.mn.us/elections-voting/election-day-voting/polling-place-rules.

AMERICAN OVERSIGHT



Voting Tip #23
Familiarize Yourself with Write-In Procedures

Upset because a candidate running unopposed in November managed to keep his DUI arrest from last year under wraps until after the primary election? In most (but not all) jurisdictions, all is not lost. A challenger may mount a write-in candidacy. Alaska Senator Lisa Murkowski is the most famous example of a write-in candidate, elected to the office via write-in after a 2010 primary election loss.

The procedures that must be followed for a write-in candidacy are controlled by state law, which means they vary widely both between states and within states (e.g., the laws governing a write-in candidacy for a county sheriff may differ from that for school board). Some states may not allow write-in candidates at all. Others will limit them to certain elections (e.g., General Elections). Check with your state or county elections office for the exact procedures that must be followed in your state.

Basically, however, a two-step process is involved, one for the candidate, one for the voter, if votes for write-in candidates will be counted:

~ Copyright by Sharon Lawrence 55 ~

AMERICAN OVERSIGHT

Process for the Candidate. In some states (e.g., Texas) a person who wants to run as a write-in candidate must file a Declaration of Write-In Candidacy. The option exists in Texas law for a person to activate his/her write-in candidacy either by paying a filing fee OR by submitting a set number of valid voter signatures on a nominating petition. Only candidates who complete one of the other of these steps may win via write-in.

Once the deadline passes for filing such a candidacy, some jurisdictions may be required by state law to print lists of declared write-in candidates and distribute them to voters with mail ballots. The list also may be required to be posted at each polling place. That's the case under Texas law for some offices, but again, state laws vary widely on this point.

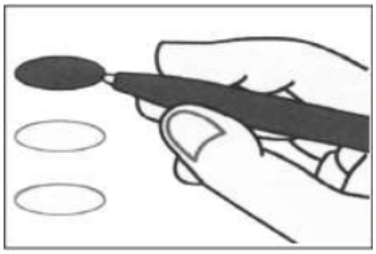
Process for the Voter. (a) If you want to vote for a write-in candidate, especially a declared write-in-candidate, check with his/her campaign to make certain you know the EXACT way to write his/her name on the ballot. State laws vary with regard to the rigidity about how the name is written. Don't risk your vote. Make certain it's written as it appears on the declaration (e.g., Joseph John Smith, not Joe Smith).

(b) On paper ballots, make certain you fill in any bubble/box that might be adjacent to the name as you've written it. (See illustration on previous page.). In some cases, your write-in vote will NOT be counted without you taking that step. If nothing else, it slows counting of the ballots if the ballot scanner notices stray marks on the ballot and kicks it out of the tabulation for special processing.

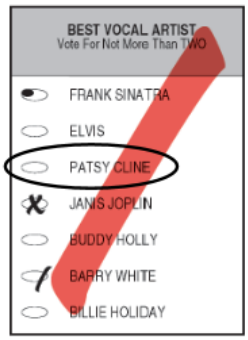
(c) Depending on the type of voting equipment used, the list of write-in candidates may be printed or required to be written on a separate ballot.

AMERICAN OVERSIGHT

Figure 2 - Examples of How to Mark a Ballot by Hand



CORRECT



INCORRECT

- Do not make any marks outside of the oval.
- Do not make any other marks on the ballot.
- Do not sign his or her name, initial, or make any other identifying marks on the ballot. Ballots with identifying marks may be rejected.

Voting Tip #24
Master the Art of Marking Your Ballot Properly

First: The Ballot

It's not only important to register to vote, but also vital that you make certain your vote counts. With the return to paper ballots and/or the rise of mail ballot elections, voters need to know how to mark their paper ballots correctly so there is no mistake about their intent or any stray mark that invalidates their vote.

Marking Devices. If you're voting at a polling place, use the marking device given to you. When voting a paper ballot outside a polling place, election officials recommend that you use a pen with black ink. As an alternative, a pen with blue ink is acceptable. DO NOT use pens with other color inks (e.g., red) or pencil as those will slow the tabulation process for your ballot.

Request Another Ballot If You Make a Mistake. If you make a mistake marking your paper ballot, ask for a replacement if at all possible. If you don't, that causes delays in the counting of your ballot as election officials must review your ballot and attempt to determine your intent. Don't leave that to chance.

Mark Your Ballot Properly. In the illustration above, the Montgomery County, MD election team illustrates the proper and improper ways to mark a ballot.

~ Copyright by Sharon Lawrence 57 ~

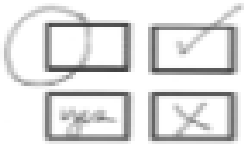
AMERICAN OVERSIGHT

Valid markings: Each of the examples provided below is a valid vote as there is a mark within the predefined target area for casting a vote.

For ballots with ovals:



For ballots with boxes:

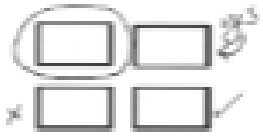


Invalid markings: Each of the examples provided below is an invalid vote as a mark does not appear within the predefined target area designated for casting a vote.

For ballots with ovals:



For ballots with boxes:

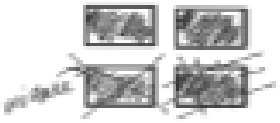


Corrections: A correction that causes a false tabulator read does not count as a valid vote.

For ballots with ovals:



For ballots with boxes:



In each example above, count the top position only.

Stray Marks: A stray mark made within a predefined target area is not a valid vote. In determining whether a mark within a predefined target area is a stray mark, the board of canvassers or election official (or board of election inspectors, when visually inspecting an absentee ballot rejected by the tabulator) shall compare the mark with other marks appearing on the ballot. Note, a cross or checkmark appearing in the predefined target area is not considered a stray mark and is a valid vote even if the voter does not consistently mark the entire ballot with a cross or checkmark.

	For ballots with ovals:	For ballots with boxes:
Candidate A		
Candidate B		
Candidate C		

In all three examples above, count the top two positions only.

As you go through the ballot, be mindful of the number of candidates that you may vote for in a given race. In local elections, for example, you may be allowed to vote for more than one

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 58 ~

candidate. You may choose to vote for fewer than the allowed number of candidates or no candidates at all, but if you vote for more than the allowed number (i.e., overvote), all votes in that race will be invalid. Do NOT write in the name of a candidate that is already on the ballot!

Shown on the previous page is part of the guidance given to Michigan poll workers to help them determine the intent of the voter if there is any question in the tabulation of a paper ballot.



At the Polling Place

Before you submit your ballot, ALWAYS check to make certain:

- ✦ You have not voted for more candidates than allowed for a given race,
- ✦ You have not missed voting for a candidate or ballot issue if you wanted to make a choice. (You don't have to vote in a race/on a ballot issue if you don't want to.) Read down each column all the way to the bottom of the page. Look at the backside of the ballot to see if any issues/races might be printed after a long column of instructions. Check the ballot against the issues/races that you marked on the sample ballot you brought with you.
- ✦ You have filled in the bubbles completely and haven't used checkmarks, circles, slash marks, or Xs to indicate your preferences.
- ✦ You have not initialed the ballot or placed any self-identifying mark on it (e.g., your address), as that will invalidate your ballot.

Voting a Mail Ballot

Once you've marked your mail ballot properly, you need to exercise extreme caution to make certain that you prepare it correctly for its return to the elections office so that, once received, it counts. Follow these steps:

AMERICAN OVERSIGHT

- ✦ Know the deadline for returning the ballot. Pay particular attention to whether the ballot (if it's to be mailed) is to be RECEIVED by a given day/time or just POSTMARKED then. If the deadline applies to when a ballot must be received, mail it at least 5 days ahead of time if mailing in-state and 7 days in advance if mailing interstate.
- ✦ Reread the instruction sheet that was sent with the ballot, if any.
- ✦ Make certain that there are no stray marks on the ballot. If there are, request another ballot.
- ✦ Do not initial the ballot or place any self-identifying mark on it (e.g., your address). That will invalidate your ballot.
- ✦ Confirm that you have not voted for more candidates than allowed for a given race,
- ✦ Look again to ensure you have not missed voting for a candidate or ballot issue. (You don't have to vote in a race/on a ballot issue if you don't want to.) Read down each column all the way to the bottom of the page to see if an issue/race might be printed after a long column of instructions. Look at the backside of the ballot to see if any issues/races were printed there. Check the ballot against the issues/races that you marked on the sample ballot you brought with you.
- ✦ Fill in bubbles for your choices completely, if you haven't already done so (No checkmarks, circles, slash marks, or Xs to indicate your preferences).
- ✦ Once you've completed that quality check, place the voted ballot into the interior (privacy) sleeve. That will be the one without the mailing address on it. Look all over that envelope to make certain that wherever you, a notary, or a witness must sign it, date it, and provide other information that is done.
- ✦ If you're voting for the first time after registering online or through your state's driver's license bureau, follow the instructions precisely for transmitting a replicate of the required voter identification.
- ✦ Seal that interior envelope (if directed to do so)[36] and place it in the exterior (carrier) envelope. That's the one with the mailing address on it.
- ✦ Again, look all over that envelope to make certain that wherever you must sign it, date it, and other provide other information such as your address, driver's license number, last four digits of your Social Security number, or voter identification number that you do so.
- ✦ If someone has helped you to mark the ballot and/or witnessed your signature, there will be a place (probably on the exterior envelope) for them to write their name, address, the date, and/or other information. Confirm that has been done!
- ✦ Write your return address clearly on the envelope.

Failure to do any of these mandated steps may invalidate your vote!

[36] New Jersey won't count your ballot if the interior envelope is not sealed! https://ucnj.org/boe/make-sure-your-vote-by-mail-ballot-is-counted-2/

AMERICAN OVERSIGHT



Voting Tip #25
Don't Forget to Apply the Appropriate Postage!

Although it seems undemocratic, voters must pay postage on most of their mail communications with election officials. Less than half of the states, according to information collected by the National Conference of State Legislatures, require that election officials provide to voters postage paid envelopes for the return of mail ballots:[37]

- Arizona
- California
- Delaware
- District of Columbia
- Hawaii
- Idaho (mail ballot districts only)
- Indiana
- Iowa
- Maryland
- Massachusetts
- Minnesota
- Missouri
- Nevada (domestic mail only)
- New Mexico

[37] https://www.ncsl.org/research/elections-and-campaigns/vopp-table-12-states-with-postage-paid-election-mail.aspx.

~ Copyright by Sharon Lawrence 61 ~

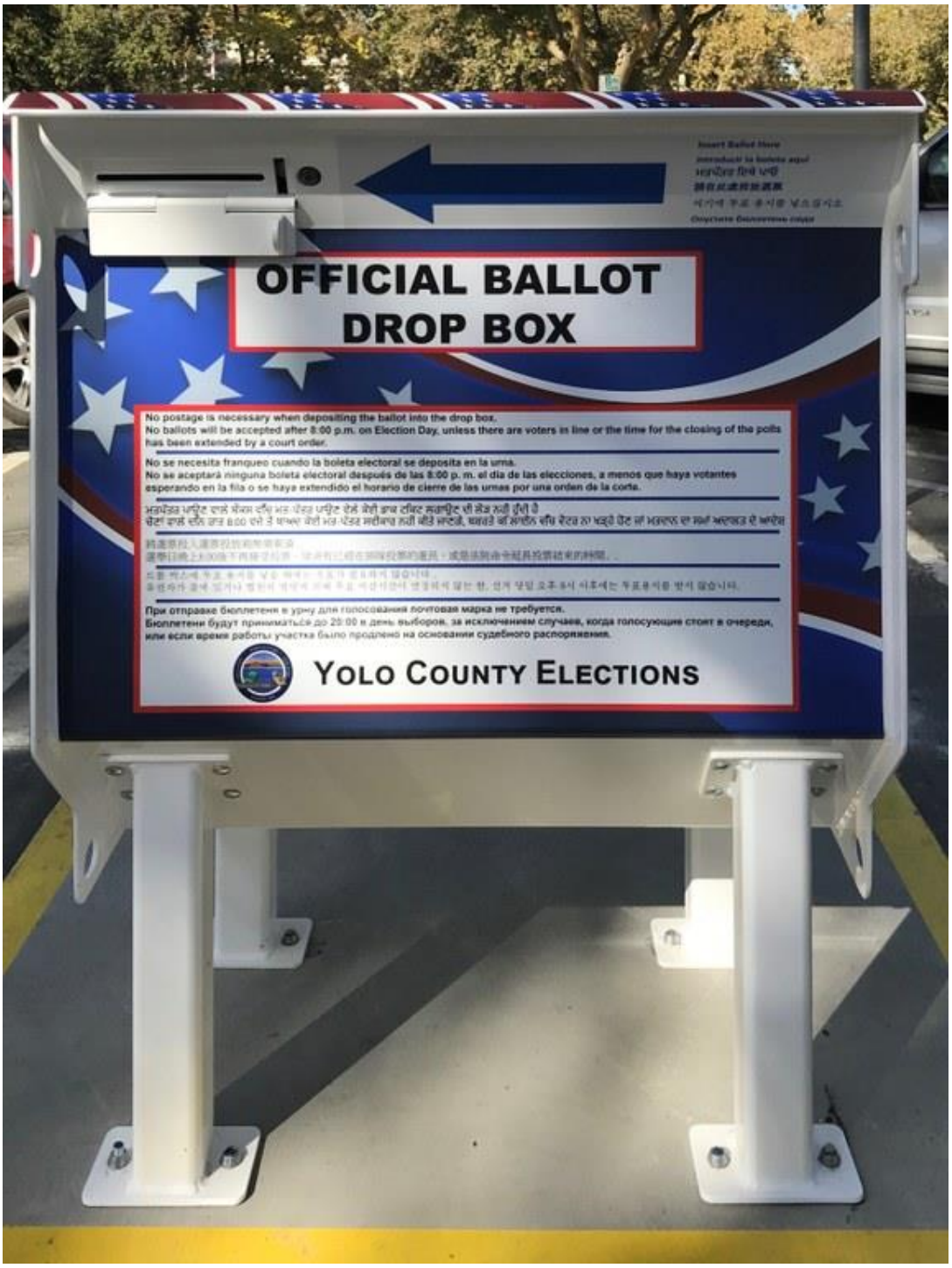
AMERICAN OVERSIGHT

- Oregon
- Rhode Island
- Virginia
- Washington
- West Virginia
- Wisconsin

Note this applies only to return of voted ballots and may not apply to other communications or transactions with the elections office (e.g., request for a mail ballot). Federal law, however, stipulates that postage will be paid for the return of ballots from military and overseas voters if mailed through the US postal system (both civilian and military versions).

~ Copyright by Sharon Lawrence 62 ~

AMERICAN OVERSIGHT



Tip #26
Pay Attention to the Restrictions on Who May Help You Vote or Handle Your Ballot in Any Way

~ Copyright by Sharon Lawrence 63 ~

AMERICAN OVERSIGHT

To guard against election fraud, states have imposed a wide variety of restrictions on who may/may not help you vote and who may/may not handle your voted ballot (e.g., to drop it off at the corner mailbox).

Given the diversity of the restrictions, it's imperative that you follow all directions listed on your voter registration materials, absentee/by mail ballot request, and voted ballot regarding who may assist you and/or handle those materials. Some general rules of thumb:

Exercise extreme caution in allowing anyone to help you vote. Residents of senior living facilities are among the groups most at risk for fraudulent assistance.

Don't allow anyone to take your application or voted ballot from you with the promise that they will deliver it/mail it for you unless they are known to you/a trusted individual.

Election materials frequently require anyone assisting a voter to write his/her name, address, and signature on the application/ballot return envelope. Read all election materials carefully and comply with any directions in this regard precisely.

Be alert for fraudulent collection sites! If you elect to place your voted ballot in a drop box (see illustration above), make certain it's an official ballot collection site. Those locations will be listed on the webpage for your local elections office or in your local newspaper. Telephone the elections office if you have any questions about a box.

If you have any questions about assistance, call your local election office for guidance!!!

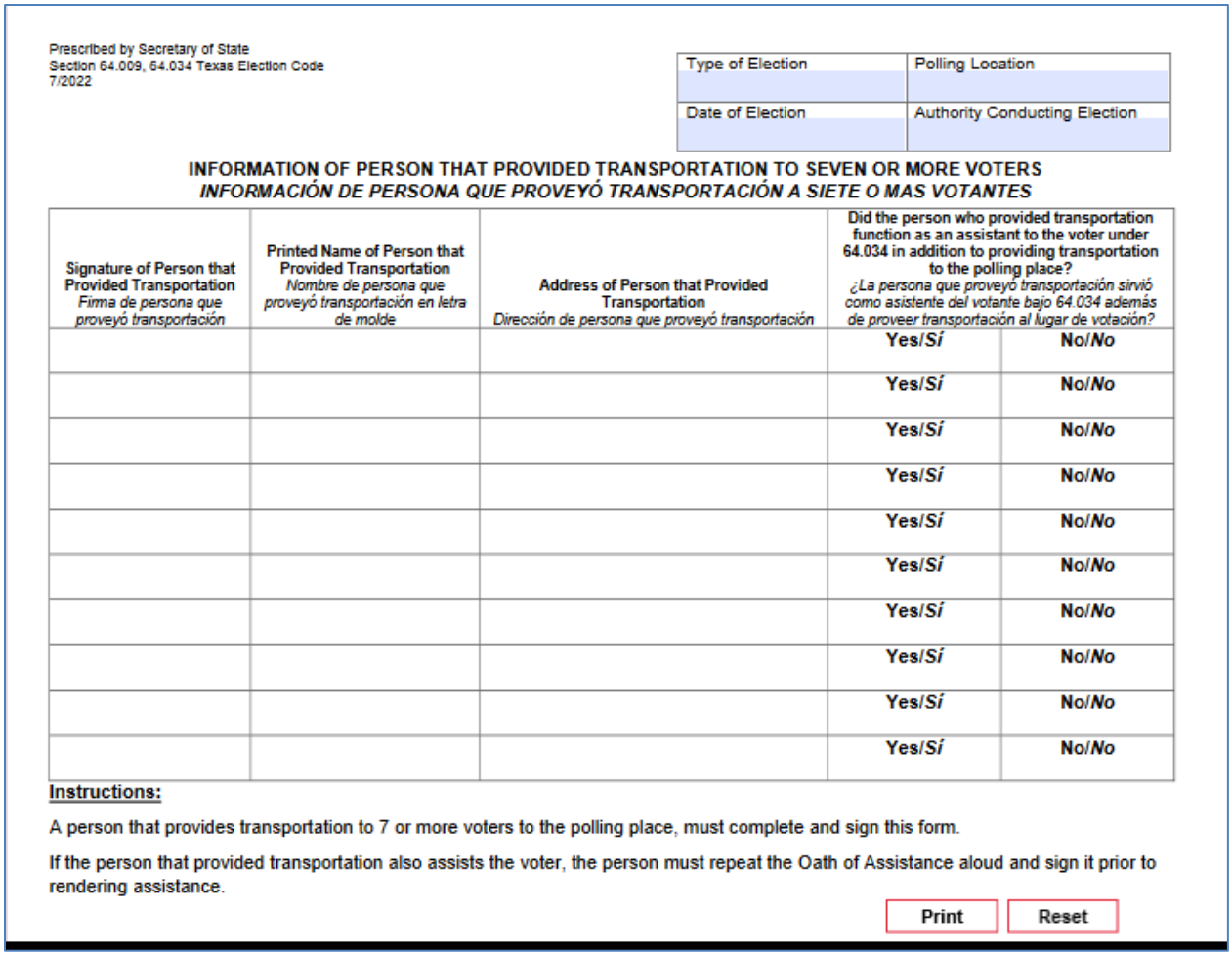
Regulations are strict! New Jersey law now states:

A person who transports a voted (completed) vote by mail ballot for someone else is considered a "Bearer." Bearers are limited to three (3) non-household ballots per election, except that an authorized bearer may transport up to five (5) ballots in an election if those voters are immediate family members residing in the same household as the bearer.

- ✦ Not to exceed (5) ballots in total for any election
- ✦ The Bearer MUST SIGN the "Bearer Portion" of the outer envelope of the ballot in the presence of the voter when taking custody of the ballot.

Any Bearer Ballots that exceed the limit must be REJECTED. If the Bearer is hand-delivering the ballot to the county Board of Elections, then he/she MUST SHOW ID AND SIGN the Bearer Book. It is against the law for anyone except you, the

AMERICAN OVERSIGHT
~ Copyright by Sharon Lawrence 64 ~



Prescribed by Secretary of State
Section 64.009, 64.034 Texas Election Code
7/2022

Type of Election	Polling Location
Date of Election	Authority Conducting Election

INFORMATION OF PERSON THAT PROVIDED TRANSPORTATION TO SEVEN OR MORE VOTERS
INFORMACIÓN DE PERSONA QUE PROVEYÓ TRANSPORTACIÓN A SIETE O MAS VOTANTES

Signature of Person that Provided Transportation *Firma de persona que proveyó transportación*	Printed Name of Person that Provided Transportation *Nombre de persona que proveyó transportación en letra de molde*	Address of Person that Provided Transportation *Dirección de persona que proveyó transportación*	Did the person who provided transportation function as an assistant to the voter under 64.034 in addition to providing transportation to the polling place? *¿La persona que proveyó transportación sirvió como asistente del votante bajo 64.034 además de proveer transportación al lugar de votación?*	
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*
			Yes/*Sí*	No/*No*

Instructions:

A person that provides transportation to 7 or more voters to the polling place, must complete and sign this form.

If the person that provided transportation also assists the voter, the person must repeat the Oath of Assistance aloud and sign it prior to rendering assistance.

Print Reset

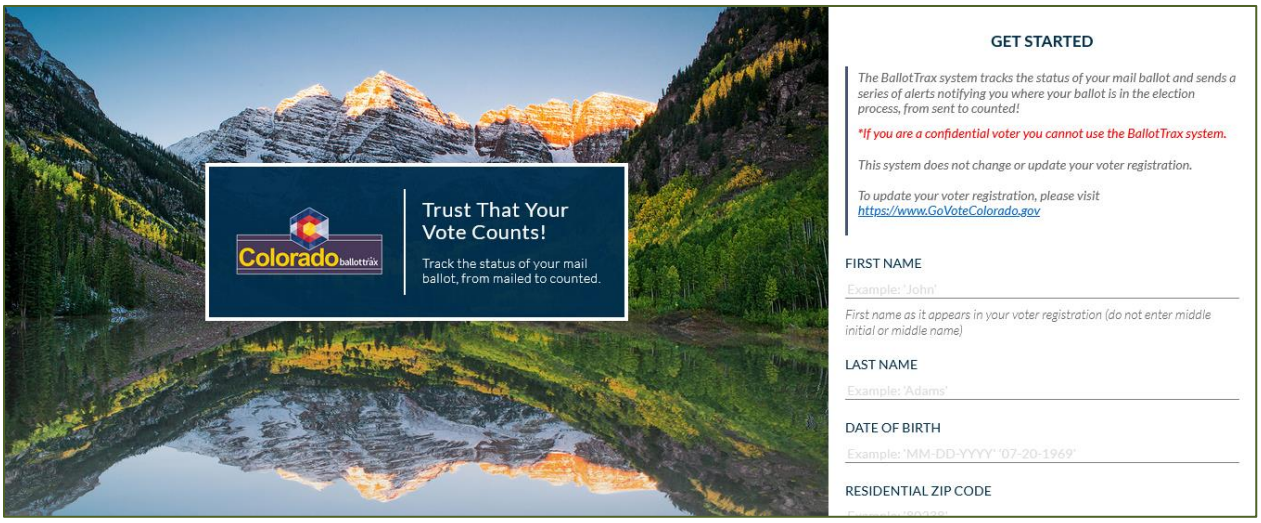
voter, to mail or transport your ballot unless the outer envelope is sealed, and the "Bearer Portion" is completed.

Rides to the Polls

Although giving rides to the polls has been one of the most traditional ways for individuals to support the democratic process, new state laws are exercising more controls over that activity as well. Texas, for example, now requires that anyone providing transportation to seven (7) or more voters must track those trips and submit the above form to local elections officials.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 65 ~



Voting Tip #27
Track Your Ballot Request or Return

~ Copyright by Sharon Lawrence 66 ~

AMERICAN OVERSIGHT



Voting Tip #28
Be Alert for Runoff Elections

In some states, the election won't be decided on November 8. If one candidate doesn't receive 50 percent of the vote plus 1 vote (or other minimum as set by state law), a runoff election will be held between the top two vote getters in the race. The races for Georgia's two US Senate seats in 2020 offer the most notable example of runoff elections and their importance.

Georgia and Louisiana subject more races to runoff requirements than other states. In Georgia, runoff elections are required for all congressional, state executive, and state legislative elections in which a candidate does not receive a majority of the votes in the general election. The top two finishers in the general election advance to the runoff.

Louisiana's use of runoff elections is more extensive. In Louisiana, all candidates running for a local, state, or federal office appear on the same ballot in either October (in odd-numbered years) or November (in even-numbered years), regardless of their partisan affiliations. If no candidate receives a simple majority of all votes cast for the office, the top two finishers, regardless of their partisan affiliations, advance to a second election in December. In that election, the candidate who receives the greatest number of votes wins.

Ten other states utilize runoff elections during the primary season when no candidate for a given political party receives the designated percentage of the vote:

- Alabama

~ Copyright by Sharon Lawrence 67 ~

AMERICAN OVERSIGHT

- ✦ Arkansas
- ✦ Georgia
- ✦ Mississippi
- ✦ North Carolina
- ✦ Oklahoma
- ✦ South Carolina
- ✦ South Dakota (i.e., congressional and gubernatorial elections only)
- ✦ Texas
- ✦ Vermont (i.e., in case of a tie)

Voters are not barred from voting in a runoff if they did not vote in the preceding primary or general election. But they may not cross over to vote in another party's primary runoff if they didn't vote in that party's primary. For the other laws and procedures governing such elections (especially as it relates to restrictions on who may/may not vote in a runoff based on their party registration or lack thereof), voters need to consult state/local election officials.[38]

[38] https://www.ncsl.org/research/elections-and-campaigns/primary-runoffs.aspx.

AMERICAN OVERSIGHT

STATE OF ALASKA
DEMONSTRATION BALLOT
November 08, 2022
General Election

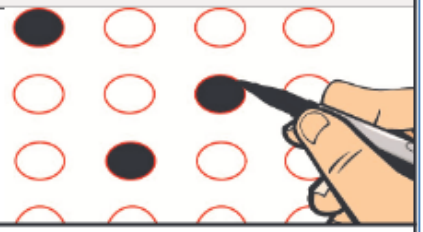
House District 1
Judicial District 4

1200

RANKED CHOICE VOTING

Instructions: Vote by ranking candidates of your choice.

- Rank as many or as few candidates as you like
- Completely fill in no more than one oval for each candidate or column
- For your 1st choice, fill in the oval in the 1st choice column
- For your 2nd choice, fill in the oval in the 2nd choice column
- For your 3rd choice, fill in the oval in the 3rd choice column, and so on
- **If you make a mistake, you can ask for a new ballot**



PLEASE NOTE: A candidate's designated affiliation does not imply that the candidate is nominated or endorsed by the political party or group or that the party or group approves of or associates with that candidate, but only that the candidate is registered as affiliated with the party or group.

United States Senator

	1st Choice	2nd Choice	3rd Choice	4th Choice	5th Choice
Heather Olson (Registered Libertarian)	○	○	○	○	○
Chick Hicks (Registered Republican)	○	○	○	○	○
Naomi Jackson (Nonpartisan)	○	○	○	○	○
Tiffany Strait (Registered AK Indep)	○	○	○	○	○
Write-in:	○	○	○	○	○

Tip #29
Understand How Ranked-Choice Voting Works

Voters in Alaska,[39] Maine,[40] and New York City,[41] among other jurisdictions, are pioneering a new way of voting in the US, i.e., Ranked-Choice Voting (also known as Instant Runoff Voting). Jurisdictions using this method present a ballot to voters similar to the one above, where they are asked to rank each candidate on the ballot in order of preference. At the close of the polls, the ballot scanners are programmed to count the first choice for each race.

If one candidate doesn't receive a majority of the voters, the votes are retabulated. This time, however, the candidate with the fewest votes is eliminated and the votes for that candidate are allocated to the voter's second choice. That process continues until one candidate has a majority of the votes.[42]

---

39 https://www.elections.alaska.gov/RCV.php.

40 https://www.maine.gov/sos/cec/elec/upcoming/rcv.html.

41 https://vote.nyc/page/ranked-choice-voting.

42 For more information, see the National Conference of State Legislatures, "Ranked-Choice Voting" (June 11, 2022); https://www.ncsl.org/research/elections-and-campaigns/ranked-choice-voting636934215.aspx.

~ Copyright by Sharon Lawrence 69 ~

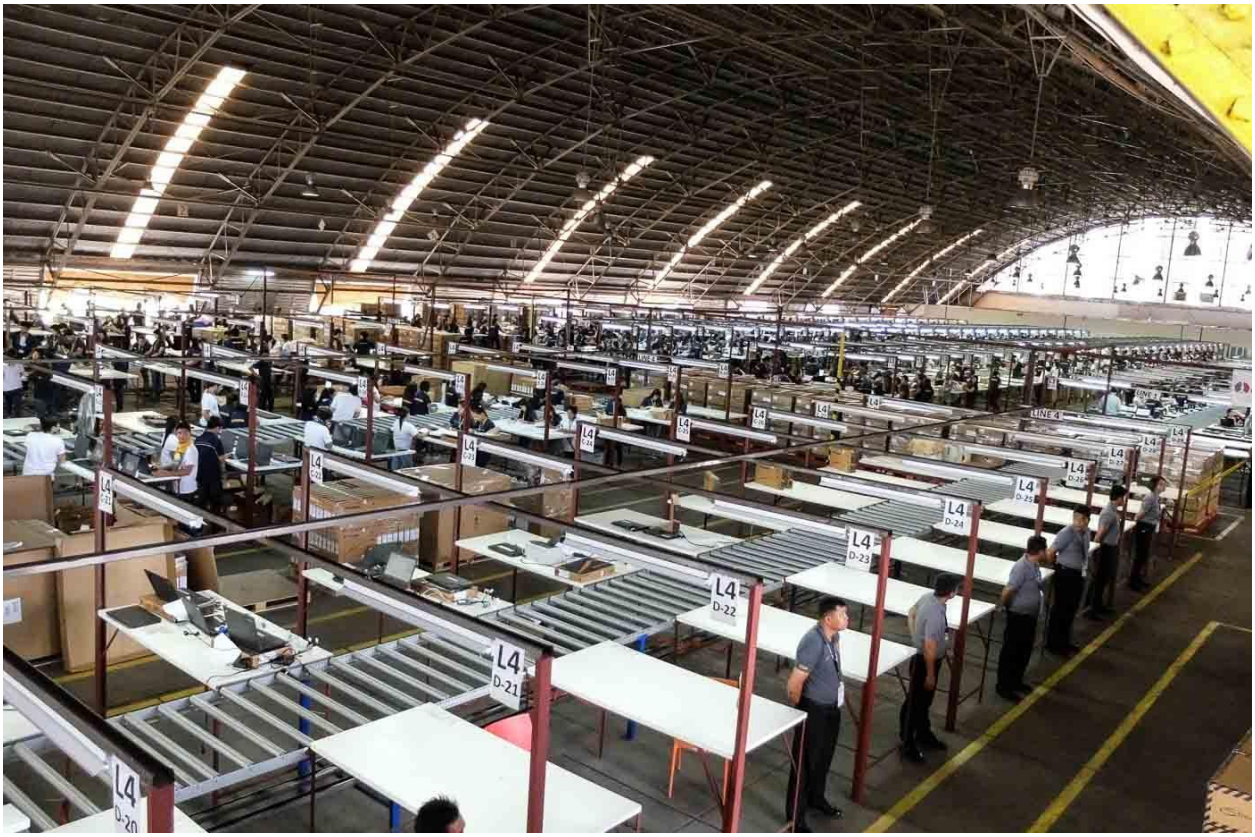
AMERICAN OVERSIGHT

As intended by the supporters, Ranked-Choice Voting puts candidates in office with a broader base of support than they might otherwise achieve, but without the additional expense and time delay of runoff elections.

Consult as well Fairvote and the Ranked Choice Voting Resource Center for more information about Ranked-Choice Voting and the jurisdictions in which it is used, https://fairvote.org/our-reforms/ranked-choice-voting and https://www.rcvresources.org/how-it-works.

~ Copyright by Sharon Lawrence 70 ~

AMERICAN OVERSIGHT



Storage of voting machines may be a state or local government responsibility. Shown above is the voting machine warehouse for the State of Connecticut.

~~~~~~~~~

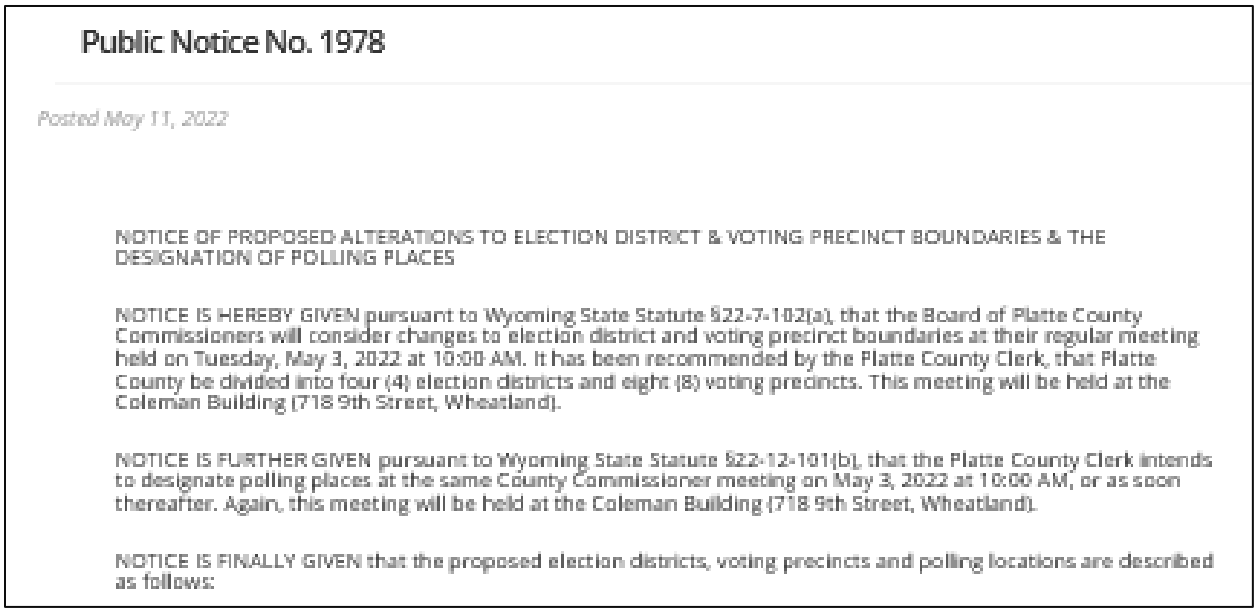
Voting Tip #30
Get Informed About Election Security Measures – Participate as a Citizen Observer

Faith in the security of the elections process is pivotal to our democracy. So that you may have confidence in the conduct and outcome of the elections, see the Appendix for a detailed overview of the multiple layers of security that apply to all steps in the election process.

But don't leave the issue just to the professionals. Know that you may play an active role in overseeing the administration of elections to ensure their accuracy and fairness.

~ Copyright by Sharon Lawrence 71 ~

AMERICAN OVERSIGHT
~~~~~~~~~



Public Notice No. 1978

Posted May 11, 2022

NOTICE OF PROPOSED ALTERATIONS TO ELECTION DISTRICT & VOTING PRECINCT BOUNDARIES & THE DESIGNATION OF POLLING PLACES

NOTICE IS HEREBY GIVEN pursuant to Wyoming State Statute §22-7-102(a), that the Board of Platte County Commissioners will consider changes to election district and voting precinct boundaries at their regular meeting held on Tuesday, May 3, 2022 at 10:00 AM. It has been recommended by the Platte County Clerk, that Platte County be divided into four (4) election districts and eight (8) voting precincts. This meeting will be held at the Coleman Building (718 9th Street, Wheatland).

NOTICE IS FURTHER GIVEN pursuant to Wyoming State Statute §22-12-101(b), that the Platte County Clerk intends to designate polling places at the same County Commissioner meeting on May 3, 2022 at 10:00 AM, or as soon thereafter. Again, this meeting will be held at the Coleman Building (718 9th Street, Wheatland).

NOTICE IS FINALLY GIVEN that the proposed election districts, voting precincts and polling locations are described as follows:

Public Oversight of the Elections Process

Take Advantage of the Opportunities for Citizens to Observe Aspects of the Elections Process. State laws consistently require that members of the public be given notice of and allowed to observe key steps in the elections process and/or comment upon them.[43] That includes:

- ✦ Designation of polling locations, which are recommended by elections staff, but must be approved by the appropriate governing body (e.g., the County Board of Commissioners/Supervisors) pursuant to the laws/regulations for approval of other government actions; and
- ✦ Pre-election testing of voting equipment for accuracy.

Look for public notices like those above and on the following page to identify opportunities for public input on or observation of elements of the election process.

Seek Designation as a Poll Watcher, Either for a Candidate, a Political Party, or a Ballot Issue. Every state has procedures in place that allow for citizens to participate as observers to ensure the integrity of elections. For more details about the myriad opportunities in your state to fulfill this vital function, consult your state or local elections office.[44]

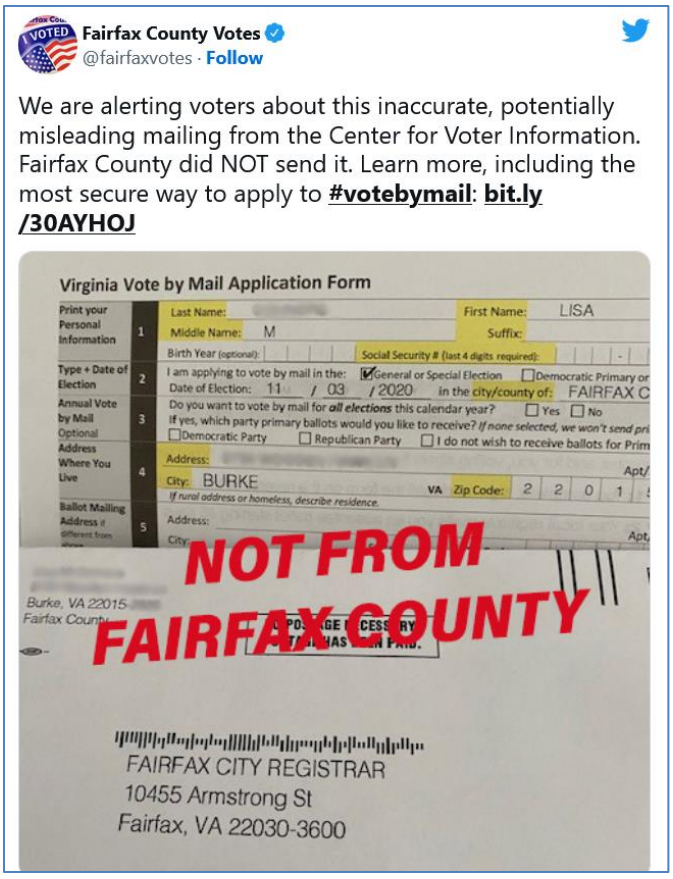
[43] Political party representatives are consistently consulted on many steps of the elections process (e.g., ballot design).

[44] The Election Assistance Commission offers additional reference works, https://www.eac.gov/election-officials/poll-watchers.

AMERICAN OVERSIGHT

Tip #31
Ensure That You Are Using Only Official Election Materials

As the competition for votes intensifies, many third-party organizations are stepping in to encourage Americans to register to vote and/or to vote by mail. Toward that end, they are distributing unsolicited absentee/by mail ballot or voter registration applications to voters.



Be cautious --- make certain that you use only official government materials (e.g., downloadable from the elections office website or mailed to you by that agency).

Laws have become increasingly detailed about the content of voter registration applications and/or mail ballot request forms. Using an unauthorized form may result in the delay or rejection of your application. Unauthorized forms also are risky to use because they might contain innocent, but nonetheless, damaging errors (e.g., the incorrect return mailing address).

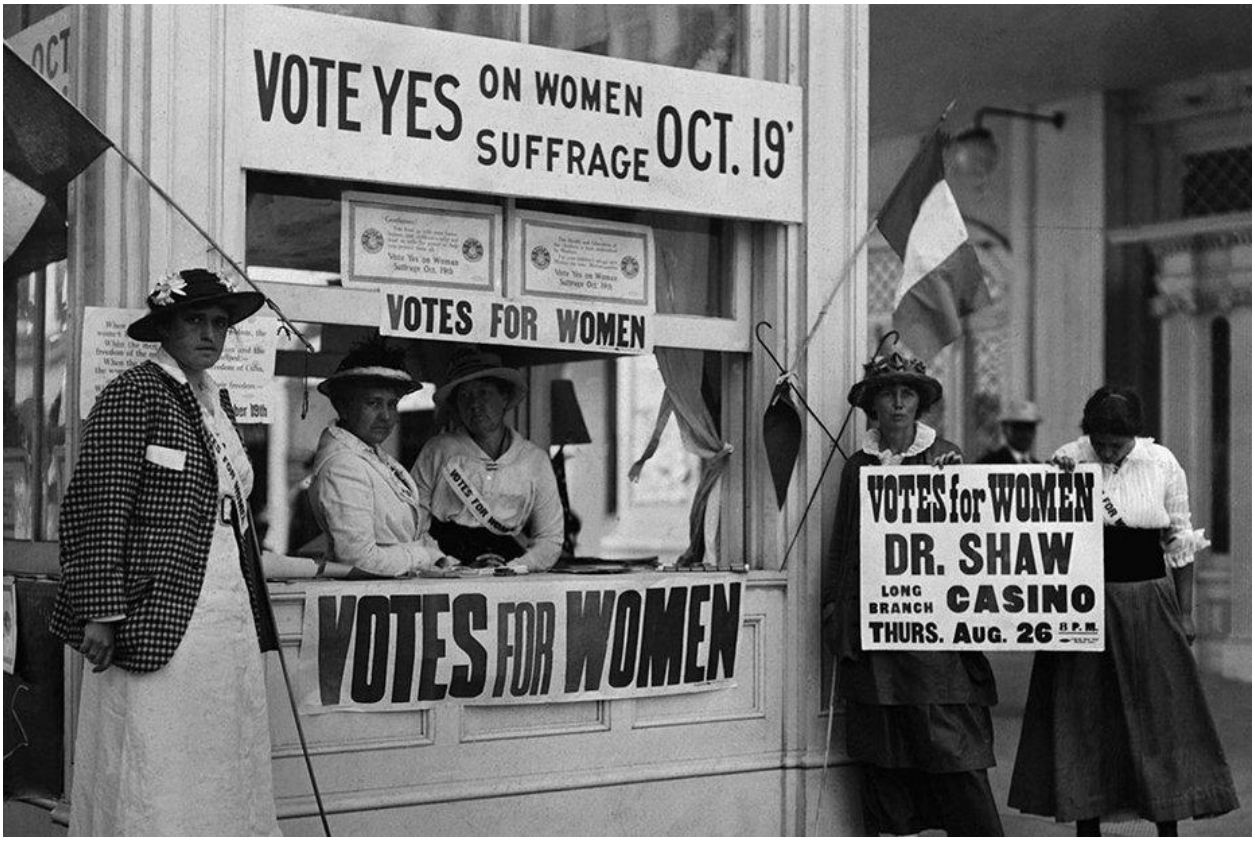
In other instances, the materials may be sent to you for a nefarious purpose (e.g., to make certain your vote doesn't count). Be cautious! Look for indications that the materials truly are official documents. Contact your elections office if you have any doubts about the authenticity of materials.

Guard Against Other Types of Fraud

A word of caution: NO election official will ask you for payment of a fee to complete any task related to voting (e.g., registering you to vote). Report any incident of this type to authorities IMMEDIATELY!

~ Copyright by Sharon Lawrence 73 ~

AMERICAN OVERSIGHT



Know Your Rights

US Constitution, Amendment 15 - Race No Bar to Vote. Ratified 2/3/1870. The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude.

US Constitution, Amendment 19 - Women's Suffrage. Ratified 8/18/1920. The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of sex.

US Constitution, Amendment 26 - Voting Age Set to 18 Years. Ratified 7/1/1971. The right of citizens of the United States, who are eighteen years of age or older, to vote shall not be denied or abridged by the United States or by any State on account of age.

Voting Rights Act of 1965. Among the key provisions of this groundbreaking legislation, Section 2 prohibits voting practices or procedures that discriminate on the basis of race, color, or membership in one of the language minority groups identified in Section 4(f)(2) of the Act.[43] Sections 203 and 204 of the Act require certain jurisdictions to provide bilingual written voting

[43] For additional details about the Act and the main Supreme Court decisions interpreting it provisions, see https://www.justice.gov/crt/voting-section.

AMERICAN OVERSIGHT

materials and voting assistance regarding covered minority languages. Another major provision of the law, Section 208, requires that voters who need assistance to vote by reason of blindness, disability, or inability to read or write may be given assistance by a person of the voter's choice (except for the voter's employer or agent of the employer or officer or agent of the voter's union).

Voting Accessibility for the Elderly and Handicapped Act (VAEHA). Since this Act's passage in 1984, states must take certain steps to make the voting process accessible to people with disabilities.[44]

Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Enacted by Congress in 1986, UOCAVA requires that states and territories allow members of the uniformed services serving away from home, their family members, and U.S. citizens who are residing outside the country to register and vote absentee in federal elections.[45]

Americans with Disabilities Act of 1990 (ADA).[46] Title II of the ADA requires state and local governments ("public entities") to ensure that people with disabilities have a full and equal opportunity to vote. The ADA's provisions apply to all aspects of voting, including voter registration, site selection, and the casting of ballots, whether on Election Day or during an early voting process.

National Voter Registration Act of 1993 (a.k.a., NVRA or "Motor Voter").[47] The National Voter Registration Act of 1993 sets forth certain voter registration requirements with respect to elections for federal office.

- ✦ Sections 5, 6, and 7 require that States offer voter registration opportunities at State motor vehicle agencies and certain State and local offices (e.g., public assistance and disability offices) and by mail-in application; and
- ✦ Section 8 mandates certain procedures election officials must follow with respect to the administration of voter registration.

The requirements of the NVRA apply to 44 States and the District of Columbia. Six States (Idaho, Minnesota, New Hampshire, North Dakota, Wisconsin, and Wyoming) are exempt from the NVRA because, on and after August 1, 1994, they either had no voter-registration requirements or had Election Day voter registration at polling places with respect to elections for federal office. American Samoa, Guam, Puerto Rico, and the US Virgin Islands are exempt from the law for the same reason.

Although the NVRA applies only to elections for federal office, States have extended its procedures to all elections.[48]

---

44 52 U.S.C. 20101 to 20107 (formerly 42 U.S.C. 1973ee to 1973ee-6).
45 52 U.S.C. 20301 to 20311 (formerly 42 U.S.C. 1973ff to 1973ff-7).
46 42 U.S.C., 12101 et seq.
47 52 U.S.C. 10301-10314, 10501-10508, and 10701-10702 (formerly 42 U.S.C. 1973 to 1973bb).
48 For more details, see https://www.justice.gov/crt/national-voter-registration-act-1993-nvra.

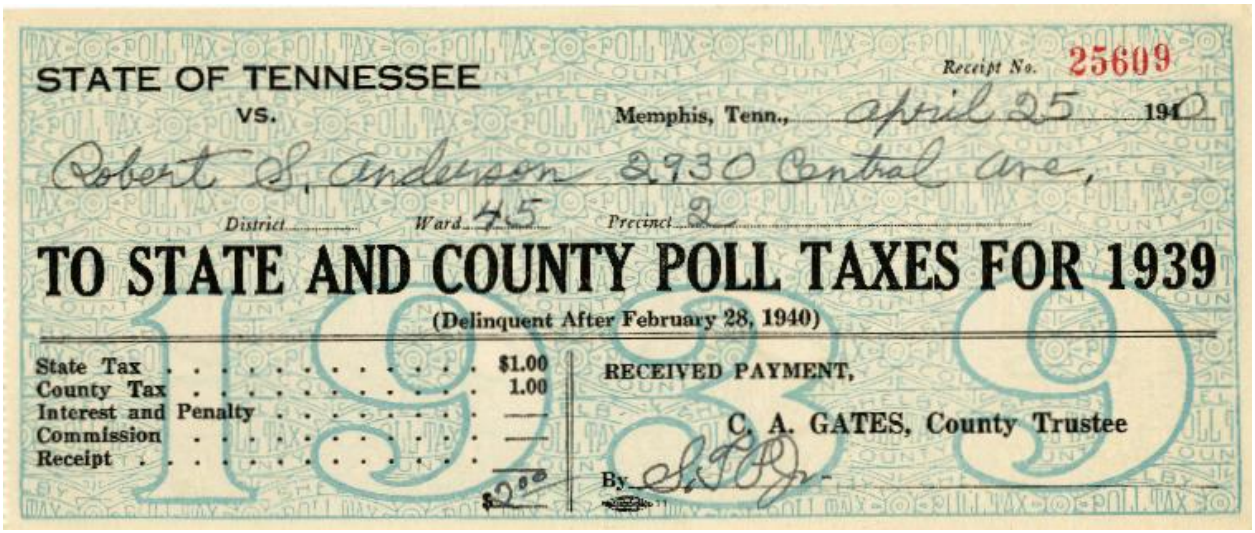
AMERICAN OVERSIGHT

Help America Vote Act (HAVA). In response to the difficulties experienced in the 2000 presidential election, Congress approved this legislation in 2002. It sets minimum standards for states to follow in several key aspects of administration of federal elections (e.g., statewide voter registration databases and voting systems). It also established a system of provisional balloting to allow voters to cast a ballot at the polling place if their eligibility was in question, pending a post-Election Day investigation of eligibility.[49]

[49] 52 U.S.C. 20901 to 21145 (formerly 42 U.S.C. 15301 to 15545).

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 76 ~



STATE OF TENNESSEE
vs.
Receipt No. 25609
Memphis, Tenn., April 25 1940
Robert S. Anderson 2930 Central Ave,
District Ward 45 Precinct 2
TO STATE AND COUNTY POLL TAXES FOR 1939
(Delinquent After February 28, 1940)
1939
State Tax $1.00
County Tax 1.00
Interest and Penalty —
Commission —
Receipt —
$2.00
RECEIVED PAYMENT,
C. A. GATES, County Trustee
By

Tip #32
Be Aware of Your Basic Rights as a Voter

As part of the "Help America Vote Act," Congress mandated that each state adopt a Voter's Bill of Rights. Florida's Voter Bill of Rights[50] reads: "Each registered voter in this state has the right to:

1. Vote and have his or her vote accurately counted.
2. Cast a vote if he or she is in line at the official closing of the polls in that county.
3. Ask for and receive assistance in voting.
4. Receive up to two replacement ballots if he or she makes a mistake prior to the ballot being cast.
5. An explanation if his or her registration or identity is in question.
6. If his or her registration or identity is in question, cast a provisional ballot.
7. Written instructions to use when voting, and, upon request, oral instructions in voting from elections officers.
8. Vote free from coercion or intimidation by elections officers or any other person.
9. Vote on a voting system that is in working condition and that will allow votes to be accurately cast.

These rights have been set forth for Massachusetts voter:

1. You have the right to vote if you are a qualified registered voter.
2. You have the right to cast your ballot in a manner that ensures privacy. You have the right to vote without any person trying to influence your vote and to vote in a booth that prevents others from watching you mark your ballot.

---

50 Florida Statutes, Sec. 101.031(2).

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 77 ~

3. You have the right to remain in the voting booth for five (5) minutes if there are other voters waiting and for ten (10) minutes if there are no other voters waiting.
4. You have the right to receive up to two (2) replacement ballots if you make a mistake and spoil your ballot.
5. You have the right to request assistance when voting from anyone of your choice. If you do not bring someone with you, you have the right to have two (2) poll workers assist you.
6. You have the right to vote if you are disabled. The polling place must be accessible, and there must be an accessible voting booth.
7. You have the right to vote if you cannot read or write or cannot read or write English.
8. You have the right to vote but must show identification if:
    a. You are a first-time voter who registered to vote by mail and did not submit identification with the voter registration form;
    b. Your name is on the inactive voter list; or
    c. Your vote is being challenged; or
    d. If requested by a poll worker.

    Acceptable forms of identification are: Massachusetts driver's license, other printed documentation containing your name and address such as a recent utility bill, rent receipt on landlord's letterhead, lease, or a copy of a voter registration acknowledgment or receipt.
9. You have the right to vote by absentee ballot if:
    a. You will be absent from your city or town on Election Day; or
    b. If you have a physical disability that prevents your voting at the polling place; or
    c. If you cannot vote at the polls due to religious belief.
10. You have the right to cast a provisional ballot if you believe you are a qualified registered voter, but a poll worker tells you that you are ineligible to vote.
11. You have the right to follow up any challenge to your right to vote through the complaint process.
12. You have the right to vote if you are not currently incarcerated for a felony conviction and have registered as a voter after your release.
13. You have the right to take this Voters' Bill of Rights or any other papers, including a sample ballot, voter guide or campaign material into the voting booth with you. Please remember to remove all papers when you leave the booth.
14. You have the right to vote at your polling place any time between 7 am and 8 pm for state and federal elections—hours may vary for local elections. If you are in line at your polling place when the polls close at 8 pm, you have the right to vote.
15. You have the right to bring your children into the voting booth with you.[51]

---

[51] https://www.sec.state.ma.us/ele/elerights/rightsidx.htm.

~ Copyright by Sharon Lawrence 78 ~

AMERICAN OVERSIGHT

Nevada adopted the following Bill of Rights for its voters.[52]

1. Each voter has the right to receive and cast a ballot that is written in a format that allows the clear identification of candidates, and accurately records the voter's preference in the selection of candidates.
2. Each voter has the right to have his or her questions concerning voting procedures answered and to have an explanation of the procedures for voting posted in a conspicuous place at the polling place.
3. Each voter has the right to vote without being intimidated, threatened, or coerced.
4. Each voter has the right to vote on Election Day if the voter is waiting in line at his or her polling place to vote before 7:00 PM.
5. Each voter has the right to return a spoiled ballot and is entitled to receive another ballot in its place.
6. Each voter has the right to request assistance in voting, if necessary.
7. Each voter has the right to a sample ballot which is accurate, informative, and delivered in a timely manner.
8. Each voter has the right to receive instruction in the use of the equipment for voting during early voting or on Election Day.
9. Each voter has the right to have nondiscriminatory equal access to the elections system, including, without limitation, a voter who is elderly, disabled, a member of a minority group, employed by the military, or a citizen who is overseas.
10. Each voter has the right to have a uniform, statewide standard for counting and recounting all votes accurately.
11. Each voter has the right to have complaints about election contests resolved fairly, accurately, and efficiently.

Virginia voters have the right to:

- ✦ Pre-register to vote by submitting a voter registration application if you are at least 16 years old but will not be 18 years old on or before the next general election.
- ✦ Register with your current address before registration records close (up to 22 days before Election Day) to vote a non-provisional ballot.
- ✦ Register in-person with your current address and vote a provisional ballot using same-day registration after registration close (21 days before Election Day) up to and including Election Day.
- ✦ Be notified if your voter registration application has been accepted or denied.
- ✦ Vote if you are registered.
- ✦ Vote absentee if you are registered to vote in Virginia.

---

[52] Nevada Revised Statutes, Sec. 293.2546.

AMERICAN OVERSIGHT

- ✦ Vote absentee in Virginia if you are a U.S. citizen overseas and your last residence in the U.S. was in Virginia, or you are a Virginia resident away in the military (or their qualifying spouse or dependent).
- ✦ Vote if you are in line by the close of polls. Polls close at 7:00 pm on Election Day.
- ✦ Be treated with courtesy and respect by election officials.
- ✦ Ask any election officer for help.
- ✦ Receive help from your own assistant or an election officer if you need help to read, complete forms, or to vote.
- ✦ Be shown how to mark and cast your ballot.
- ✦ Bring your child (age 15 or younger) into the voting booth.
- ✦ Have a ballot brought to your vehicle instead of entering the polling place or early voting location if you are 65 years of age or older -- or have a disability.
- ✦ Request to receive your absentee ballot electronically to mark your ballot using an electronic ballot-marking tool, if you are print disabled.
- ✦ Use an accessible voting machine when voting in person at your polling place or early voting site, if you have a disability and prefer that option.
- ✦ Write in the full name of a candidate if the candidate of your choice is not listed on the ballot (except in party primaries).
- ✦ Ask for a new ballot if you want to change your vote *before* you cast it.
- ✦ Vote a regular ballot if you arrive at your polling place without acceptable ID, but sign an ID Confirmation Statement affirming your identity.
- ✦ Vote a provisional ballot if your name does not appear on the voter list and you believe it should, if you utilize the same-day registration process, or if you forgot to bring an acceptable ID and refuse to sign an ID Confirmation Statement.
- ✦ Receive notice of the time and place of the Electoral Board meeting to determine if your provisional ballot will be counted and, if applicable, the deadline by which any required documents must be submitted (such as acceptable ID).
- ✦ Be present when the Electoral Board meets to determine if your provisional ballot will be counted (attendance is not required for your ballot to be counted).[53]

A Closer Look at Discrimination and Voter Intimidation

To help that state's voters protect their rights, Pennsylvania's Secretary of State offers the following guidance on voter intimidation and discriminatory conduct.

> Any activity that threatens, harasses, or intimidates voters outside the polling place, inside the polling place, at secure ballot receptacles, at mailboxes, or at county

[53] https://www.elections.virginia.gov/casting-a-ballot/voter-rights/

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 80 ~

election offices is illegal. This includes any activity intended to, or having the effect of, interfering with any voter's right to vote….

Federal and State Laws

- Election officials and poll workers are prohibited under federal law from discriminating against voters based on race, ethnicity, national origin, language, disability, or religion, or from allowing any discriminatory conduct by private actors to affect voters. These protections are detailed in the United States Constitution, the Voting Rights Act, and the Americans with Disabilities Act.
- Election officials and private citizens are prohibited from conspiring with others to deprive a voter of their right to vote.
- Under state law, it is illegal for any person or corporation to directly or indirectly practice intimidation or coercion to induce or compel a person to vote or refrain from voting for a particular candidate or on a particular political issue through:
  - Use of force;
  - Violence;
  - Restraint;
  - Infliction of injury, damage, harm, or loss; or
  - Threatened infliction of injury, damage, harm, or loss.
- Under state law, it is illegal for a person or corporation to use abduction, duress, coercion, or any other forcible or fraudulent means to impede, prevent or otherwise interfere with a person's right to vote.
- Election officials, including poll workers, cannot knowingly refuse the vote of a registered voter.[54]

In addition, the Secretary of State offers these examples of voter intimidation and discriminatory conduct.

- Aggressive or threatening behavior inside or outside the polling place.
- Blocking or interfering with access to:
  - The entrance or exit to the polling place;
  - Accessible accommodations for voters with disabilities;
  - Voter sign-in tables or voting booths/voting machines;
  - Secure ballot receptacles provided by the County; or
  - Mailboxes provided by the US Postal Service (USPS).
- Direct confrontation or questioning of voters, including asking voters for documentation or proof of eligibility when none is required.
- Disrupting voting lines inside or outside of the polling place, at a secure ballot receptacle provided by the County, or USPS mailboxes.
- Disseminating false or misleading election information, including information on voting eligibility, polling place procedures, polling place hours, or voting methods.

---

[54] https://www.vote.pa.gov/Your-Rights/Pages/Voter-Intimidation.aspx.

AMERICAN OVERSIGHT

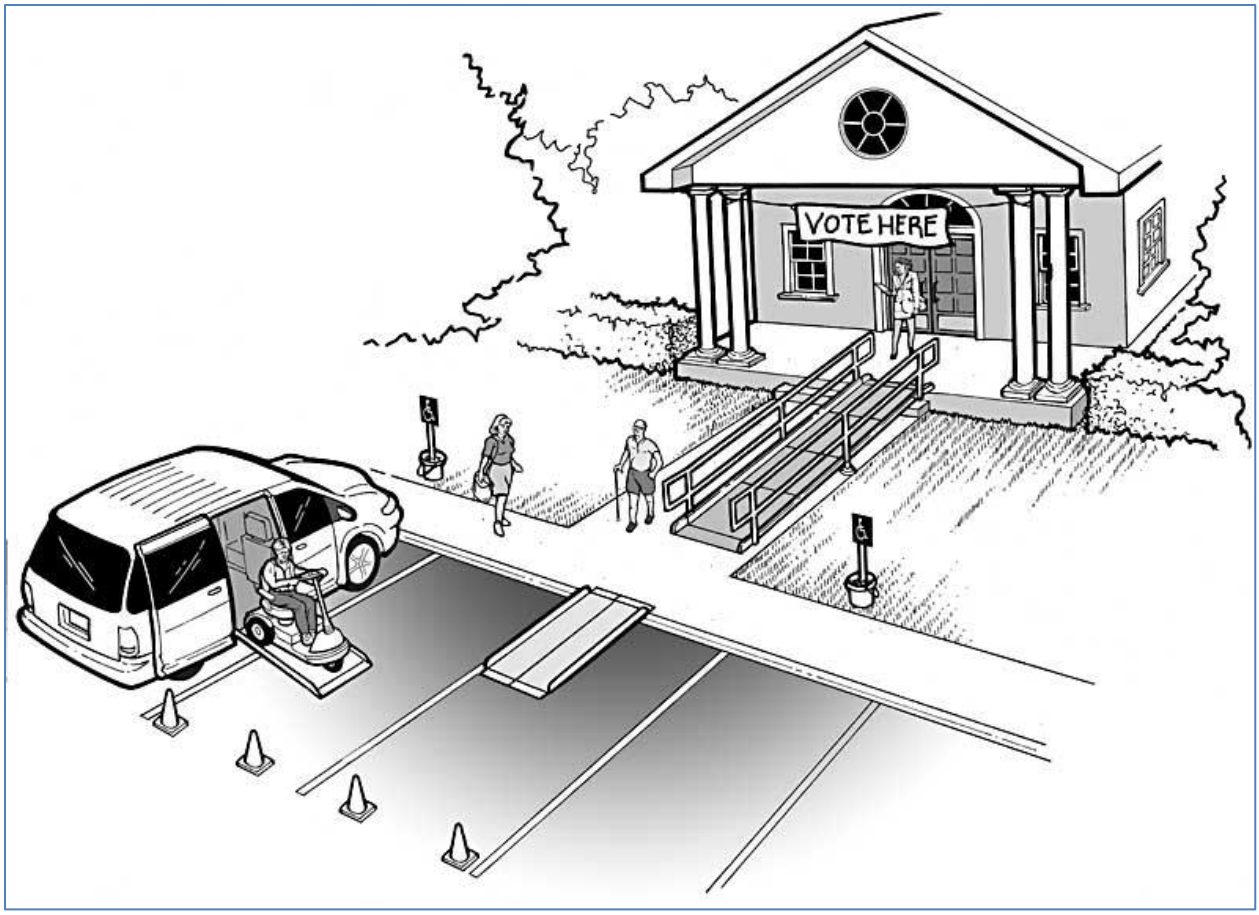
~ Copyright by Sharon Lawrence 81 ~

- ✦ Election workers treating a voter differently in any way based on race, ethnicity, national origin, language, disability, or religion.
- ✦ Aggressive or threatening brandishing of weapons.
- ✦ Photographing or videotaping voters to intimidate them.
- ✦ Posting signs in the polling place, at a secure ballot receptacle, or at a USPS mailbox to intimidate voters or drive support for a candidate.
- ✦ Routine and frivolous challenges to voter's eligibility by election workers or private citizens that are made without a stated good faith basis.
- ✦ Questioning voters about citizenship, criminal record, or political choices.
- ✦ Using raised voices, screaming, yelling, or shouting; use of insulting, offensive, or threatening language; chanting taunts; or threatening songs inside the polling place.
- ✦ Vandalism of polling places, polling place equipment/materials, secure ballot receptacles, or mailboxes.
- ✦ Verbal or physical confrontation of voters by persons dressed in official-looking uniforms.
- ✦ Falsely representing oneself as an election official or law enforcement authority.
- ✦ Violence or using the threat of violence to interfere with a person's right to vote.
- ✦ Interfering with or violating a voter's right to a secret ballot at any point in the process.[55]

[55] https://www.vote.pa.gov/Your-Rights/Pages/Voter-Intimidation.aspx.

~ Copyright by Sharon Lawrence 82 ~

AMERICAN OVERSIGHT



Tip #33
Right to Accessible Polling Places and Voting Equipment

Pursuant to multiple federal statutes, voters are guaranteed the right to accessible polling places and voting equipment.

Accessible Applications, Ballots, and Instructions

Montana voters with physical impairments have the option to request an electronic ballot.[56] To help them participate most effectively in the elections process, the state also makes available online audio and large-print versions of the Voter Information Pamphlet; a Braille version is available upon request.

Rhode Island assists voters with physical limitations by offering absentee/by mail ballots in Braille, tactile format, or large print.

---

56 https://sosmt.gov/elections/disabilities.

~ Copyright by Sharon Lawrence 83 ~

AMERICAN OVERSIGHT



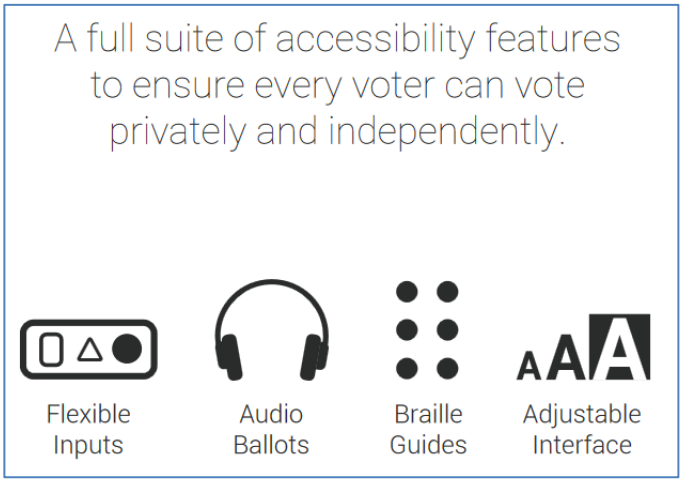
Accessible Polling Places & Voting Equipment

As elections officials contract for polling places, those locations must now meet standards for:

- Parking,
- Passenger drop-off areas,
- Exterior routes to accessible entrances,
- Polling place entrances,
- Route from entrance into voting area,
- The voting area, and
- Elevators, lifts, and ramps.[57]

Curbside Voting. Voters with temporary or permanent impairments may not need to enter the polling place.[58] Many states (but not Indiana) allow for curbside voting. Parking for that service should be marked clearly outside the polling place.

That allows the voter to remain in the vehicle while a team of election workers brings all the items needed for voting to them. Privacy is strictly observed during this process.



Accessible Voting Equipment

Not only must the polling place accommodate the needs of those with physical limitations, but the voting equipment must also as well. In federal elections, every polling place must have at least one voting system that allows voters with disabilities to vote privately and

[57] US Department of Justice, Civil Rights Division, Disability Rights Section, "ADA Checklist for Polling Places," https://www.ada.gov/votingchecklist.htm#toc17.

[58] See North Carolina's

~ Copyright by Sharon Lawrence 84 ~

AMERICAN OVERSIGHT

independently. Usually, this is a machine that can read the ballot to a voter (for people with vision disabilities or dyslexia) and let an individual vote by pushing buttons (for people with mobility disabilities).

In Chicago polling places, the Election Board offers various tools to help voters with different physical abilities.[59] Each facility used as a polling place must meet the following standards:

> Alternate Entrance Signs, where needed, will be posted at polling places to direct voters with disabilities to the entrance that offers the easiest access.
>
> Doorbells are offered outside entrances to polling places with heavy doors. When voters ring the bells, a judge of election will come and open the door for the voter.
>
> Threshold Ramps are placed at polling places where the door threshold is such that a voter in a wheelchair may have difficulty entering. The threshold ramps will make for easier entry into the polling place.

Once inside the polling place, Chicago voters with disabilities will have these tools at their disposal:

> An Information and Services Notice ("Need Help Voting?" sign) is printed in large type. This Notice lists services and rules for voters who may receive assistance while voting. This Notice is to be posted on a wall in each polling place.
>
> Ballot Marker Grippers allow voters to easily hold the marking pens for paper ballots.
>
> Large Ballot Viewers are magnifying lenses designed to enlarge the print on the paper ballots to assist voters who require assistance to read the names of offices, candidates, and referenda.
>
> Wheelchair accessible voting booths are available in each polling place. Voters who are unable to stand for long periods of time also may use this unit and a provided chair.
>
> Audio Controller Unit and Audio Ballots in the touchscreen voting units allow a visually impaired voter to hear the balloting instructions, offices, candidates, and referenda and allow them to make their choices and cast their ballot by use of a handheld controller unit and supplied headphones. This controller can also be affixed to the arm of a chair or wheelchair by using the Velcro straps attached to the unit.
>
> Audio Visual Ballots on the touchscreen allow voters who may have difficulty moving their arms or dexterity issues to use the keypad and the headphones but also see the ballot being displayed on the screen.

---

59 https://chicagoelections.gov/en/accessibility-voters-with-disabilities.html.

AMERICAN OVERSIGHT

> Sip-and-Puff Devices on the touchscreen voting units can be used in conjunction with the audio controller. The sip and puff device will navigate the voter through the audio ballot.
>
> Assisted Voting is available to those who designate a trusted family member or other friend to help the voter cast a ballot. An affidavit must be signed by the voter and the person assisting. The voter also may request the assistance of two judges of election, one from each major political party, to help the voter cast a ballot.

Other Accommodations

Election officials may take other steps to ensure that voters with disabilities or physical limitations have a positive voting experience. Poll workers in Connecticut have special guidance on how they may assist voters who have difficult standing in line have several options.

> …..[T]hey can approach the Moderator of the polling place and request that they be allowed to move to the front of the line due to the challenges imposed by standing. Moderators should accommodate them. A voter may also ask the Moderator to direct them to a chair they can use. Election officials are encouraged to provide suitable seating to accommodate said requests. The voter's place in line should be held and the Moderator or a poll worker will let them know when it is time for them to vote.[60]

Texas election officials also are empowered (encouraged) to accommodate the needs of those with challenges standing for long periods. Per statute,

> An election officer may give voting order priority to individuals with a mobility problem that substantially impairs the person's ability to move around.
>
> - A person assisting an individual with a mobility problem may also, at the individual's request, be given voting order priority….
> - Voters who wish to be given voting order priority, and be accepted for voting before others in line to vote at that polling place, may indicate this to any election officer serving at the polling place. The presiding election judge will determine whether the voter and the voter's assistant, if applicable, will be brought forward to the front of the line.[61]

---

60 https://portal.ct.gov/SOTS/Election-Services/Voter-Information/Voters-with-Disabilities-Fact-Sheet.

61 https://www.sos.texas.gov/elections/forms/pol-sub/7-33f.pdf.

~ Copyright by Sharon Lawrence 86 ~

AMERICAN OVERSIGHT



نموذج

SAMPLE

بطاقة اقتراع رسمية
الانتخابات البلدية التمهيدية
الثلاثاء ٣ أغسطس ٢٠٢١
مقاطعة وين، ميشيغن
مدينة ديربورن، قلم اقتراع ١

قسم مقترحات القوانين

مدينة

مقترح «أي»

هل توافق على مراجعة وتحديث ميثاق مدينة ديربورن الذي تم تبنيه، بصيغته المعدلة، في ٦ نوفمبر ٢٠٠٧، من قبل لجنة منتخبة في انتخابات لاحقة؟

- ○ Yes نعم
- ○ No لا

تجديد الضريبة العقارية (ميليج) لتمويل مكتبات ديربورن لـ٦ سنوات

منذ عام ٢٠١١، سمح ناخبو ديربورن بتخصيص ١ مل لتمويل خدمات المكتبات. هذا الـ١ مِل يولّد سنوياً حوالي ٣,٧٠٠,٠٠٠ دولار، أو ٦٠ بالمئة تقريباً من ميزانية تشغيل المكتبات.
إذا لم يتم تجديد هذا الميليج، فسوف ينجم عن ذلك تخفيضات ضرورية في المرافق والمواد والبرامج والخدمات، وكذلك خسارة إضافية من تمويل الولاية بمقدار ٧٠٠,٠٠٠ دولار على الأقل.

هل تستمر بلدية ديربورن -وفقاً لقانون الولاية (أم سي أل) ٣٩٧,٢٠١ في فرض ضريبة لا تتجاوز واحد دولار لكل ١٠٠٠ دولار من القيمة الضريبية (١مِل) لمدة لا تزيد عن ٦ سنوات، والتي سيتم تخصيصها بشكل صارم لتأمين تكاليف التشغيل ورأسمال أنظمة المكتبات؟

- ○ Yes نعم
- ○ No لا

مدينة

سباق المجلس البلدي

لا تصوّت لأكثر من سبعة مرشحين!

○ Ziad Abdulmalik	زياد عبد الملك
○ Robert A. Abraham	روبرت أبراهام
○ Jonathon Akkari	جوناثان عكاري
○ Saeid Mashgari Alawathi Formerly known as Said Ali Mashgari	سعيد مشغري الأواثي (المعروف سابقاً باسم سعيد علي مشغري)
○ Kamal Alsawafy	كمال الصوافي
○ Houda Berri	هدى بري
○ Erin Byrnes	إيرن بيرنز
○ Silvio Davis	سيلفيو دافيس
○ Kamel Elkadri	كامل القادري
○ Lola Elzein	لولا الزين
○ Gary Enos	غاري إنوس
○ Khodr Farhat	خضر فرحات
○ Mustapha Hammoud	مصطفى حمود
○ Leslie C. Herrick	ليزلي هيريك
○ Sam Luqman	سام لقمان
○ Khalil Othman	خليل عثمان
○ Ken Paris	كين باريس
○ Michael T. Sareini	مايكل سرعيني

سباقات غير حزبية

مدينة

سباق رئاسة البلدية

لا تصوّت لأكثر من مرشح واحد!

○ Hussein Berry	حسين بري
○ Susan A. Dabaja	سوزان دباجة
○ Abdullah Hammoud	عبدالله حمود
○ Jim Parrelly	جيم باريللي
○ Thomas Patrick Tafelski	توماس باتريك تافيلسكي
○ Kalette Shari Willis	كاليت شاري ويليس
○ Gary Woronchak	غاري وورنتشاك

Dearborn, Michigan's Arabic Ballot – August 2021 City Elections

~~~~~~~~~~

Tip #34
Right to Bilingual Election Materials

~ Copyright by Sharon Lawrence 87 ~

AMERICAN OVERSIGHT
~~~~~~~~~~

In 2019, 26.9 million people in the U.S. had limited English proficiency, and 67.8 million people spoke a language other than English at home.[62] To ensure that those who are citizens may participate fully in the elections process, Section 203 of the Voting Rights Act requires states and political subdivisions to provide bilingual voting materials to individuals who speak Alaska Native, American Indian, Asian, and Spanish languages. That general mandate applies to jurisdictions if:

- More than five (5) percent of the voting age citizens (or in excess of 10,000 voting age citizens) exhibit limited-English proficiency;[63] and
- The rate of total voting age citizens that exhibit limited-English proficiency and have less than a fifth-grade education is higher than the national rate.

Not only must ballots be bilingual, so too must be all envelopes, instructions, and voter guides produced in conjunction with covered elections. Unwritten languages require oral translation as well. Polling places in affected jurisdictions must make available bilingual voting assistants.

The list of covered jurisdictions for 2022 elections, published in the December 8, 2021 **Federal Registe**r, includes 331 local governments and 3 states.[64] Of the 331 jurisdictions, 68 are newly covered under Section 203. That list includes localities in:

Alaska
Arizona
California
Colorado
Connecticut
Florida
Georgia
Hawaii
Idaho
Illinois
Kansas
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Nebraska
Nevada
New Jersey
New Mexico
New York
Ohio
Oklahoma
Pennsylvania
Texas
Utah
Virginia
Washington
Wisconsin. [23]

California, Florida, and Texas are covered statewide for Hispanic language minorities.

---

62 Election Assistance Commission, "Language Access Program Checklist," https://www.eac.gov/sites/default/files/languages/Language_Access_Program_Checklist.pdf.

63 That is, do not ''speak or understand English adequately enough to participate in the electoral process."

64 Coverage is updated every five years.

23 https://www.justice.gov/crt/page/file/1460416/download.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 88 ~



Tip #35
Right to Cast a Provisional Ballot
In Case of Questions about Eligibility

If you appear at the polls and a question is raised about your eligibility to vote, DO NOT despair or walk away. You may still vote.

As part of the Help America Vote Act passed in 2002, Congress established a provisional ballot process whereby a voter may vote, despite the fact his/her eligibility might be in question, by providing additional information to support the claim of a right to vote. Staff experts for the National Conference of State Legislatures explain the purpose of the provision ballot:

> Provisional ballots ensure that voters are not excluded from the voting process due to an administrative error. They provide a fail-safe mechanism for voters who arrive at the polls on Election Day[24] and whose eligibility to vote is uncertain.[25]

A sworn affidavit submitted by the voter, furnishing details supporting his/her claim of eligibility, and the marked ballot (referred to as a provisional ballot) are segregated for review by election officials. If the questions about voter eligibility may be resolved within the deadline set by law, the ballot will be processed and the votes on it included in the totals for that election.

---

[24] Or during the Early Voting period.

[25] https://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx.

~ Copyright by Sharon Lawrence 72 ~

AMERICAN OVERSIGHT

Ohio election officials describe the process to their voters in this way.

> **What scenarios would require me to cast a provisional ballot?**. Any of the following scenarios would require you to cast a provisional ballot on Election Day:
>
> - ✦ Your name does not appear on the official poll list for that precinct, or an election official asserts that you are not eligible to vote or is unable to determine your eligibility;
> - ✦ You are unable to provide or do not have the required proof of identity, which includes an Ohio driver's license or state identification card, military identification, other current and valid photo identification, or a current (within the last 12 months) utility bill, bank statement, government check, paycheck or other government document (other than a notice of voter registration mailed by a board of elections) that shows the voter's name and current address;
> - ✦ Your name appears on the official poll list for that precinct as having already requested an absentee ballot;
> - ✦ Your name is marked on the poll list or signature book with a notation that certain registration mailings have been returned as undeliverable;
> - ✦ Your voter registration has been challenged and/or a hearing on a challenge to your eligibility as an elector has been postponed until after Election Day; or
> - ✦ Your signature, in the opinion of the precinct officers, does not match the signature on your registration form.
>
> **Name changes:** If you have changed your name but have not yet updated your voter registration, you may vote a regular ballot rather than a provisional ballot as long as you have not moved to a new address outside of your voting precinct. You must provide elections officials proof of a legal name change such as a marriage license or a court order that includes your current and prior names. At your polling location or designated vote center, you will simply be asked to complete a change of name form.[26]

The Pennsylvania Secretary of State's Office lists the common reasons why a voter might be directed into the provisional voting process:

- ✦ Your name was not in the poll book or supplemental poll book. For example, you reported to the wrong precinct; or You did not report a recent change in residence to the county election office.
- ✦ You are required to show identification, but cannot show that identification at that time.
- ✦ Your eligibility was challenged by an election official.

---

[26] https://www.ohiosos.gov/elections/voters/provisional-voting.

AMERICAN OVERSIGHT

- ✦ You were issued but did not successfully vote an absentee or mail-in ballot and you do not surrender your ballot at the polling place to be spoiled.[27]
- ✦ You returned a completed absentee or mail-in ballot that was rejected by the county board of elections and you believe you are eligible to vote.
- ✦ There is a special court order with respect to your registration status.
- ✦ There is a special court order related to extending the hours of voting.
- ✦ You believe that you are registered in a political party, but your voter record indicates otherwise (for primary elections only).[28]

Upon completion of that affidavit described above, a voter will receive a written notice informing him/her that they will be notified by mail within 30 days of the election if their provisional ballot was counted, and if was not counted, the reason why.

PLEASE take the opportunity to cast a provisional ballot if asked to do so. This is NOT a wasted effort. According to Los Angeles County election officials, "**Past election records show that on average 85-90% of provisional ballots are valid and counted."**[29]

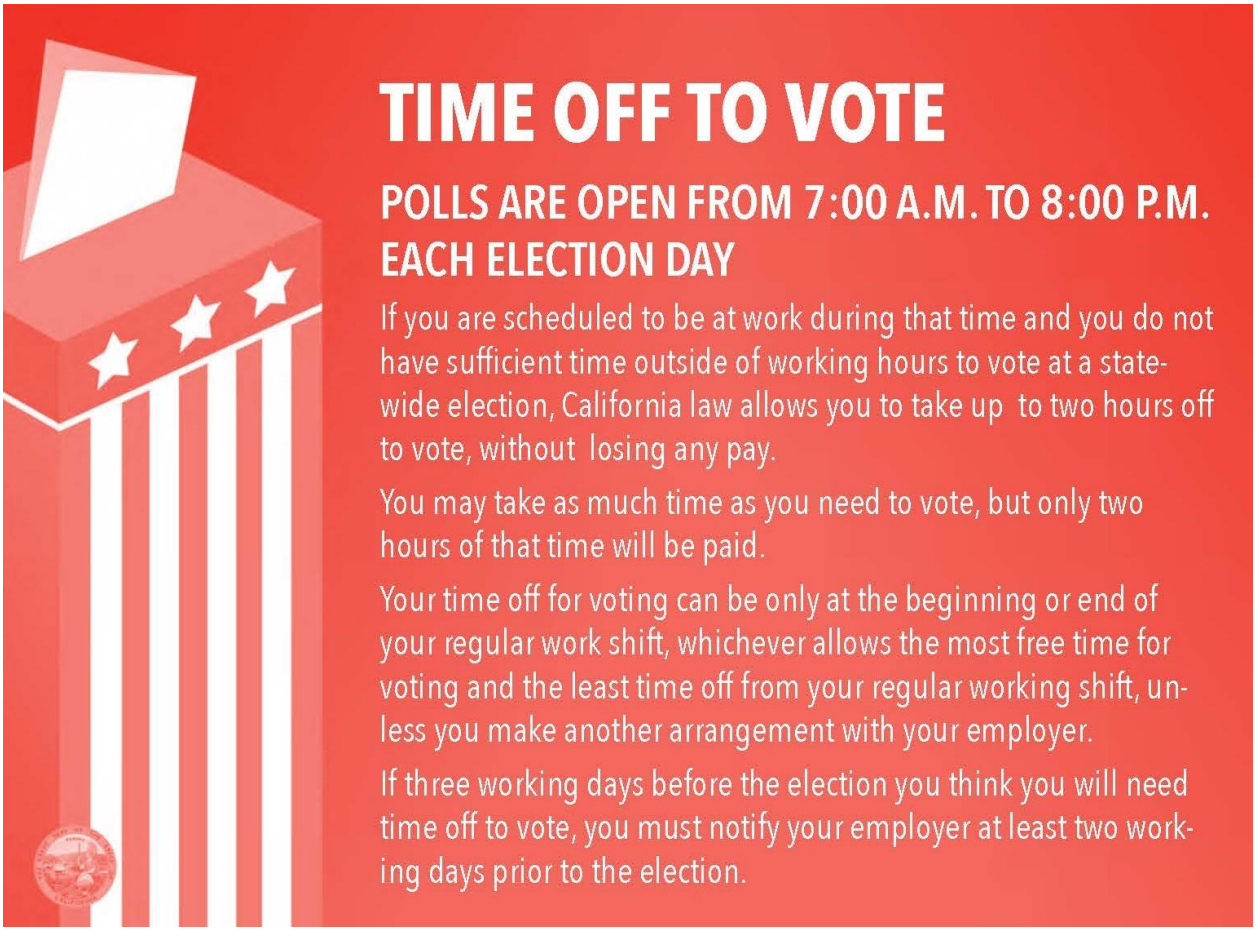
2727 Spoiled, in layman's terms, means cancelled.

28 https://www.vote.pa.gov/Voting-in-PA/Pages/Voting-by-Provisional-Ballot.aspx.

29 https://www.lavote.gov/home/voting-elections/voting-options/voting-in-person/provisional-voting.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 74 ~



Tip #36
Right to Take Time Off From Work to Vote

In a number of states, Election Day is a holiday for schools and state workers. Several states, however, have stepped up to encourage/facilitate Election Day turnout by mandating that private sector employers allow time off for voting as well. Those laws vary by:

- How much time off is required by law,
- If advance notice of the planned absence is required to receive legal protection,
- If the time off is at the employer's expense or unpaid,
- If proof of voting is required, and
- Whether or not an employer is banned from disciplining or firing an employee for a voting related absence.[30]

See the attached chart for a state-by-state breakdown of the laws in this regard.

[30] https://www.workplacefairness.org/voting-rights-time-off-work.

~ Copyright by Sharon Lawrence 75 ~

AMERICAN OVERSIGHT



Tip #37
Right to Vote If In Line When Poll Closing Time Arrives

No matter how LONG the line waiting to vote might be, all states require that the polls remain open until each and every voter in line at the deadline (e.g., 7 p.m.) is allowed to vote. DO NOT LEAVE!

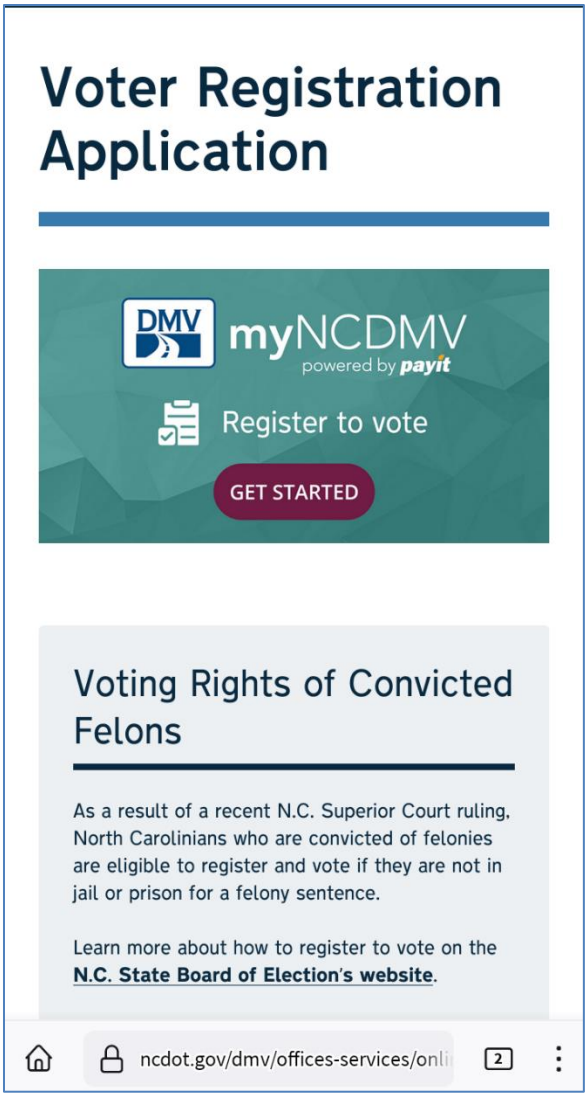
In line, however, does not include being in the parking lot waiting for a space to open or walking up from the bus stop. So don't delay! Take that poll closing time seriously!

~ Copyright by Sharon Lawrence 76 ~

AMERICAN OVERSIGHT

Tip #38
Right to Vote If Incarcerated, But Not Yet Convicted; Right to Vote After Felony Conviction & Sentence Completion

No federal laws or regulations govern the restoration of voting rights if revoked for conviction of a crime. States are free, therefore, to handle the matter in any manner they see fit. They also set the rules for the procedures which incarcerated, but not yet convicted, individuals must follow to exercise their voting rights.



Treatment of Those Accused or Convicted of State Crimes. States take one of the following approaches in addressing the voting rights of individuals convicted of a crime:

- ✦ Permanent disenfranchisement for all people with felony convictions;
- ✦ Permanent disenfranchisement for at least some people with criminal convictions;
- ✦ Voting rights restored upon completion of sentence, including prison, parole, and probation;
- ✦ Voting rights restored for those on probation or parole who have not been incarcerated during the last five years;
- ✦ Voting rights restored automatically after release from prison; and
- ✦ No disenfranchisement for people with criminal convictions (i.e., Maine, Vermont, and the District of Columbia only).[31]

As might be expected, this is an exceptionally complex process. Individuals seeking to restore their eligibility to vote should consult with corrections and elections officials for guidance.[32]

---

[31] https://www.brennancenter.org/our-work/research-reports/can-people-convicted-felony-vote-felony-voting-laws-state.

[32] In addition to the Brennen Center, organizations working with affected individuals include:
- ✦ Campaign Legal Center, https://campaignlegal.org/restoreyourvote, and
- ✦ Restoration of Rights Project, https://restoration.ccresourcecenter.org.

~ Copyright by Sharon Lawrence 77 ~

AMERICAN OVERSIGHT

Treatment of Those Convicted of Federal Crimes. Although the restoration process is governed by state law, shortly after taking office President Biden issued an Executive Order titled "Promoting Access to Voting."[33] In part, that Order requires the Attorney General (AG) to take four important actions to ensure access, for people in federal custody or under federal supervision, to voter registration and educational materials on voting:

First, the AG must "provide educational materials related to voter registration and voting and, to the extent practicable, to facilitate voter registration, for all eligible individuals in the custody of the Federal Bureau of Prisons….The educational materials should also notify individuals leaving Federal custody of the restrictions, if any, on their ability to vote under the laws of the State where the individual resides and, if any such restrictions exist, the point at which the individual's rights will be restored under applicable State law."

Second, the AG must establish procedures to ensure that contracts with jails housing federal detainees require those jails provide educational materials on voter registration and voting, and to facilitate voting by mail, to the extent practicable and appropriate.

Third, the AG must coordinate with the Office of Probation and Pretrial Services in the Administrative Office of U.S. Courts to provide voter educational materials to all eligible individuals under supervision, and to facilitate their voter registration and voting.

Fourth, the AG must take appropriate steps to support formerly incarcerated individuals in obtaining identification that satisfies voter identification laws in the state of their residence.

For an overview of the Florida law on this point, see https://escambiavotes.gov/frequently-asked-questions-faq-for-persons-convicted-of-a-felony.

[33] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/03/07/executive-order-on-promoting-access-to-voting/.

AMERICAN OVERSIGHT

Tip #39
Right of Designated At Risk Individuals to Request That Certain Identifying Information Be Withheld from the Public

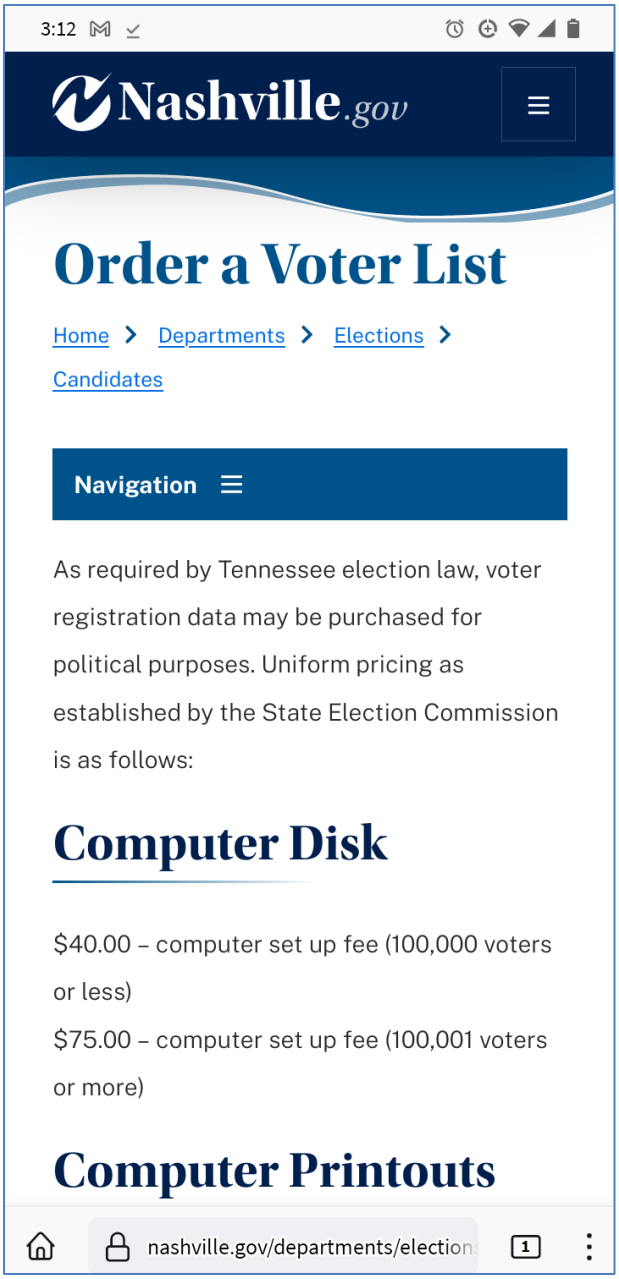
Many people may not know that most of the information provided on a voter registration application and their voting history may be distributed to willing buyers.

Per state law, the Virginia Department of Elections may sell to qualified buyers lists of:

- ✦ Newly registered voters,
- ✦ Registered voters,
- ✦ Those who voted absentee in a given election,
- ✦ Those who voted (regardless of method) in a given election,
- ✦ Vote history,[34] and
- ✦ Voter registration updates.[35]

To protect those in certain sensitive occupations (e.g., judges) or at risk of physical harm (e.g., domestic violence), states have established procedures to prevent disclosure of voter information.

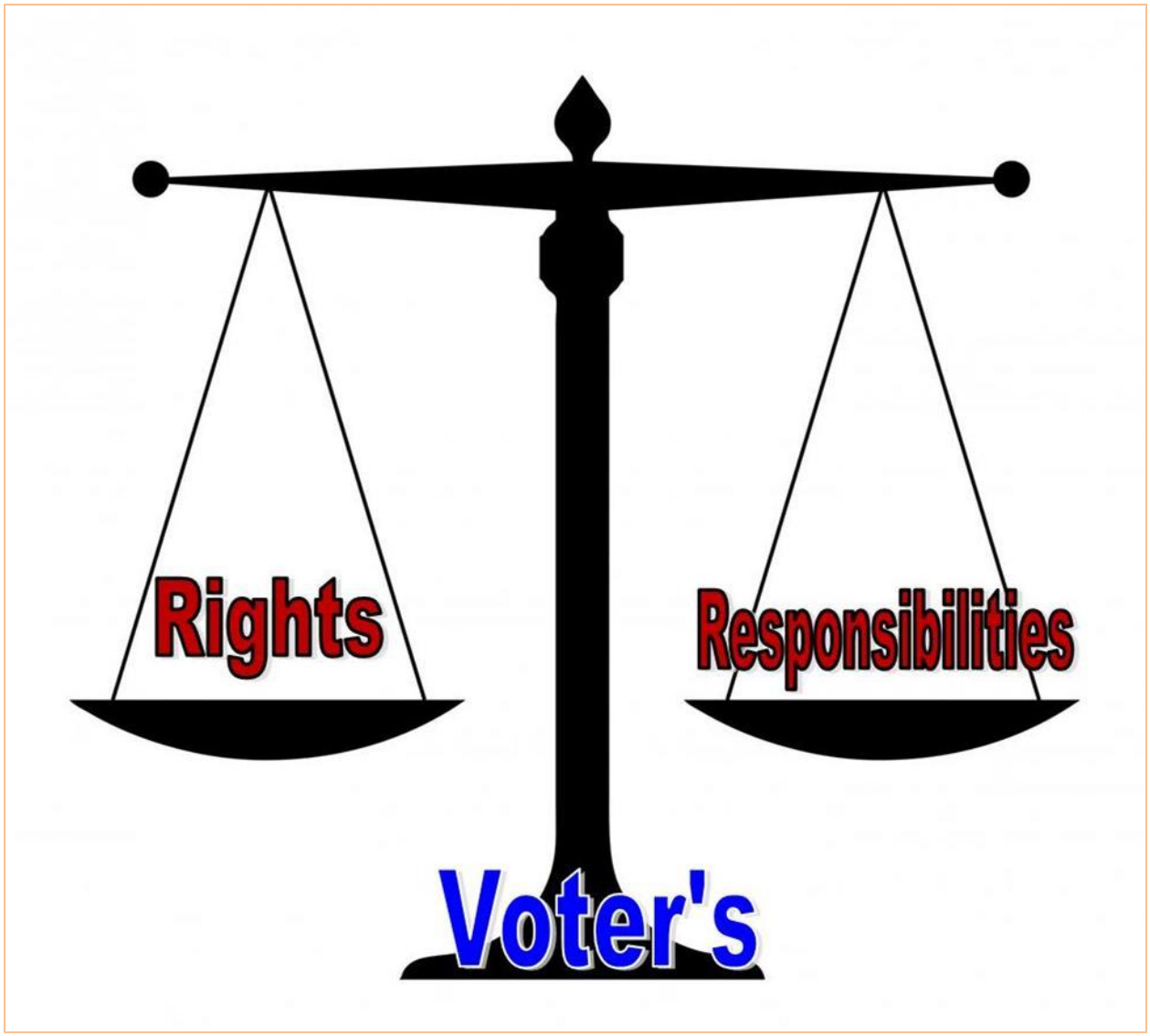
Address confidentiality laws vary according to who they cover and the process by which the confidentiality may be pursued.[36] Consult your state/local elections officials for information on the proper procedure to follow to claim this vital protection.



[34] Who voted in a given election in a specific jurisdiction over a four-year period.
[35] https://www.elections.virginia.gov/candidatepac-info/client-services.
[36] For a brief discussion of the address confidentiality laws and programs available in each state, if any, see https://www.addressconfidentiality.com/states.

~ Copyright by Sharon Lawrence 79 ~

AMERICAN OVERSIGHT



Graphic: Courtesy Supervisor of Elections, Okeechobee County, FL

Know Your Responsibilities

~ Copyright by Sharon Lawrence 80 ~

AMERICAN OVERSIGHT



Tip #40
Respect the Rights of Voters and the Elections Process

Tip #22 discussed the laws and policies governing polling place conduct from the perspective of the voter. A broader set of laws and procedures are in place, however, to protect the integrity of the elections process, both inside and outside a polling place. These are applicable not only to voters but other interested parties (e.g., media or public opinion polling organizations).

For federal elections, the Federal Bureau of Investigation (FBI) has offered this overview of federal election crimes.

> While individual states and localities have the constitutional authority and responsibility to manage elections and have their own election laws, an election crime becomes a federal crime when one or more of the following occurs:
>
> - A ballot includes one or more federal candidates
> - Election or polling place officials abuse their office
> - The conduct involves false voter registration
> - The crime is motivated by hostility toward minority protected classes
> - The activity violates federal campaign finance law
>
> Examples of federal election crimes include, but are not limited to:
>
> - Giving false information when registering to vote
> - Voting more than once
> - Changing ballot markings or otherwise tampering with ballots
> - Compensating voters
> - Threatening voters with physical or financial harm
> - Intentionally lying about the time, manner, or place of an election to prevent qualified voters from voting
> - Political fundraising by federal employees

~ Copyright by Sharon Lawrence 81 ~

AMERICAN OVERSIGHT

- ✦ Campaign contributions above legal limits
- ✦ Conduit contributions
- ✦ Contributions from foreign or other prohibited sources
- ✦ Use of campaign funds for personal or unauthorized purposes

….The following activities are not **federal** election crimes; however, states have their own election laws…

- ✦ Giving voters rides to the polls or time off to vote
- ✦ Offering voters a stamp to mail a ballot
- ✦ Making false claims about oneself or another candidate
- ✦ Forging or faking nominating petitions
- ✦ Campaigning too close to polling places

The Elections Department for the City/County of San Francisco summarizes these applicable laws and procedures as follow.

Observation is Permissible. In general, all election processes are open to public observation and all San Francisco residents, members of the media, campaigns, candidates, and any other interested parties are encouraged to observe these processes. However, all observers must comply with local, state, and federal law, and campaign supporters, media staff, and members of the public alike are expected to conduct their observation activities in a safe and respectful manner.[37]

Exit Polling is Permissible. Exit polling is the surveying of voters after they leave a voting site. This activity is generally permissible, along with the taking of voluntary "ballot selfies" and similar recordings, because state law allows a voter to "voluntarily disclose how he or she voted if that voluntary act does not violate any other law." Per current California Secretary of State guidance, members of the media and others conducting exit polls may do so at least 25 feet from a voting area, in a quiet, non-disruptive manner.

Corruption of the Voting Process is Prohibited. Corruption of the voting process, which constitutes criminal activity, can take many forms, including but not limited to voter fraud, bribery, and interference with election processes or voter rights. Per state law, any person who engages in corruption of the voting process may be guilty of a felony; violations are subject to fine and/or imprisonment.

ANY OF THE FOLLOWING ACTIVITIES ARE PROHIBITED:

- ✦ Commit or attempt to commit election fraud.

[37] To help potential observers familiarize themselves with election processes and observation guidelines, the Department publishes the **Observer Guide** that includes observer rights and responsibilities, as determined by the California Secretary of State and California Elections Code, and a description of observable activities that take place before, on, and after Election Day. **Guide to Observing Elections Processes**, https://sfelections.sfgov.org/sites/default/files/Documents/candidates/November2022_ObserverGuide.pdf.

AMERICAN OVERSIGHT

- ✦ Provide or attempt to provide compensation or bribery to induce a person to vote or refrain from voting.
- ✦ Illegally vote or attempt to vote or aide another to vote when not entitled to vote.
- ✦ Engage in electioneering, voter obstruction, or unauthorized photography at voting sites.
- ✦ Challenge a person's right to vote or prevent voters from voting or delay the process of voting.
- ✦ Fraudulently advise any person that he or she is not eligible to vote or is not registered to vote.
- ✦ Attempt to ascertain how a voter voted their ballot.
- ✦ Possess or arrange for anyone to possess a firearm in or near a polling place (with some exceptions).
- ✦ Appear or arrange for anyone to appear in police or security guard uniform (with some exceptions).
- ✦ Tamper or interfere with any component of a voting system or alter the returns of an election.
- ✦ Forge, counterfeit, or tamper with the returns of an election.
- ✦ Tamper with, destroy, or alter any polling list, official ballot, or ballot drop box.
- ✦ Display any unofficial ballot collection container that may deceive a voter into believing it is an official ballot drop box.
- ✦ Tamper or interfere with copy of the results of votes cast.
- ✦ Coerce or deceive a person who cannot read or an elder into voting contrary to their intent.
- ✦ Act as an election officer if you are not an election officer.[38]

[38] https://sfelections.sfgov.org/permissible-and-prohibited-election-activities.

AMERICAN OVERSIGHT



Voting Tip #41
Respect the Rights of Candidates To Communicate with Voters

It's that time of year when campaign signs start popping up everywhere. And since you really, really dislike the candidate for XYZ county office, you may be tempted to help his campaign sign disappear at 2 a.m. after you've been lifting a few with your buddies at the local brew pub. DON'T EVEN THINK ABOUT DOING THAT!

Defacing, damaging, or stealing campaign sights is illegal in virtually every community in the US. If you don't like that candidate, help get out the vote for his/her opponent; don't violate the spirit of our democracy by impairing the ability of candidates to communicate with the voters.

For an overview of each state' laws on campaign signs, see https://www.findlaw.com/legalblogs/law-and-life/is-it-illegal-to-steal-or-vandalize-political-signs/.

~ Copyright by Sharon Lawrence 84 ~

AMERICAN OVERSIGHT



Voting Tip #42
Comply with Government Regulations for the Display of Campaign Signage

Many Americans love to show their support for candidates by placing campaign signs on their property. Although that's a welcomed activity, such displays of support are typically regulated by state and/or local governments. The City of Creve Coeur, Missouri, for example, imposes the following guidelines on campaign signage:

> In addition to signs that are allowed during the rest of the year, temporary election signs and other non-commercial signs are allowed during election season. These additional temporary signs are regulated by the city's zoning ordinance to ensure pedestrian and vehicular safety are not hindered due to improper sign placement. Regulations include:
>
> - Signs are not permitted within the public right-of-way. The right-of-way is typically 10 to 15 feet back from the curb. (See illustration above)
> - If a sidewalk is present, signs must be placed on the property side (signs may not be placed between the sidewalk and roadway).
> - Signs may be posted starting 45 days before the election.
> - Signs must be removed no later than 10 days after the election.
> - Signs are only permitted with the property owner's permission.
> - Signs may be single- or double-faced, but no sign face may exceed six square feet on residential property or 12 square feet on commercial property.

~ Copyright by Sharon Lawrence 85 ~

AMERICAN OVERSIGHT

- ✦ The number of additional signs per lot may not exceed the number of candidates or propositions on the ballot.
- ✦ Signs may not be attached to utility poles.
- ✦ When placing an election sign, do not block access or visibility of pedestrian or vehicular traffic.
- ✦ When installing an election sign, take care not to block the access or visibility of pedestrian or vehicular traffic.[39]

[39] https://www.crevecoeurmo.gov/255/Election-Sign-Regulations.

~ Copyright by Sharon Lawrence 86 ~

AMERICAN OVERSIGHT

Tip #43
Report Election Fraud or The Violation of Voting Rights

Federal, state, and local government officials are charged with protecting the voting rights of individuals.

At the federal level, the US Department of Justice, Civil Rights Division's Voting Section enforces the civil provisions of a wide range of federal statutes that protect the right to vote including: the Voting Rights Act, the National Voter Registration Act, the Uniformed and Overseas Citizens Absentee Voting Act, the Help America Vote Act, and the Civil Rights Acts. Among other things, collectively, these laws:

- Bar election practices that have either a discriminatory purpose, based on race or membership in a minority language group, or a discriminatory result, with members of racial or language minority groups having less opportunity than other citizens to participate in the political process;
- Prohibit voter intimidation;
- Provide that individuals who need assistance in voting because of disability or illiteracy may obtain assistance from a person of their choice;
- Mandate that election officials have in place accessible election machines for voters with disabilities;
- Require provisional ballots for voters who assert they are eligible but whose names do not appear on poll books;
- Establish standards for the distribution of absentee ballots to service members, their family members and U.S. citizens living abroad;
- Require states to ensure that citizens can register through drivers' license offices, public assistance and disability services offices, other state agencies, and through the mail; and
- Set requirements regarding maintaining voter registration lists.

GENERAL INFORMATION
CIVIL RIGHTS DIVISION
VOTING SECTION

CONTACT

Toll-free - (800) 253-3931
Telephone - (202) 307-2767

To report a Federal Voting Rights Violation

Mailing Address
U.S. Department of Justice
Civil Rights Division
Voting Section
950 Pennsylvania Avenue NW
4CON 8th Floor
Washington, DC 20530
voting.section@usdoj.gov

Violations of voting rights may be reported to the Justice Department online, https://civilrights.justice.gov/report.

The Civil Rights Division's Criminal Section enforces federal criminal statutes that prohibit voter intimidation and voter suppression based on race, color, national origin or religion.

~ Copyright by Sharon Lawrence 87 ~

AMERICAN OVERSIGHT

Several non-profit organizations also offer substantial support to voters experiencing or witnessing voting rights violations, including:

- ✦ Election Protection;[40] and
- ✦ Lawyers Committee for Civil Rights Under Law.[41]

States also set standards for the conduct of elections to protect the integrity of the process. Missouri Statutes, Section 115.637, for example, declares it shall be a misdemeanor, punishable by imprisonment of not more than one year or by a fine of not more than two thousand five hundred dollars or by both such imprisonment and fine:

> (1) Stealing or willfully concealing, defacing, mutilating, or destroying any sample ballots that may be furnished by an organization or individual at or near any voting place on election day….,
> (2) Printing, circulating, or causing to be printed or circulated, any false and fraudulent sample ballots which appear on their face to be designed as a fraud upon voters;
> (3) Purposefully giving a printed or written sample ballot to any qualified voter which is intended to mislead the voter;
> (9) Any person having in his or her possession any official ballot, except in the performance of his or her duty as an election authority or official, or in the act of exercising his or her individual voting privilege;
> (10) Willfully mutilating, defacing, or altering any ballot before it is delivered to a voter;
> (13) On the part of any election judge, or party watcher or challenger, furnishing any information tending in any way to show the state of the count to any other person prior to the closing of the polls;
> (14) On the part of any voter, except as otherwise provided by law, allowing his or her ballot to be seen by any person with the intent of letting it be known how he or she is about to vote or has voted, or knowingly making a false statement as to his or her inability to mark a ballot;
> (15) On the part of any election judge, disclosing to any person the name of any candidate for whom a voter has voted….

---

[40] https://www.lawyerscommittee.org/project/election-protection.
For assistance,
1. Call:
   - ✦ (866) OUR-VOTE;
   - ✦ (888) VE-Y-VOTA (Spanish/English);
   - ✦ (844) YALLA-US (Arabic/English);or
   - ✦ (888) API-VOTE (English, Mandarin, Cantonese, Korean, Vietnamese, Tagalog, Urdu, Hindi and Bengali)
2. Text MYVOTE to (866) 687-8683;
3. Visit their Facebook or Twitter pages;
4. Use Messenger at @866ourvote; or
5. WhatsApp (http://wa.me/18666878683).

[41] https://www.lawyerscommittee.org/project/voting-rights-project.

~ Copyright by Sharon Lawrence 88 ~

AMERICAN OVERSIGHT

Governor / Lt. Governor

Republican Candidates - Vote for 1

(37 of 37 election day precincts reported)

Name	Party	Early Voting	Election Day	Mail-In Ballot / Provisional	Total	Percentage
Dan Cox and Gordana Schifanelli ✔	Republican	427	3,507	535	4,469	61.85%
Robin Ficker and LeRoy F. Yegge, Jr.	Republican	37	208	154	399	5.52%
Kelly Schulz and Jeff Woolford	Republican	235	1,572	452	2,259	31.26%
Joe Werner and Minh Thanh Luong	Republican	11	51	37	99	1.37%

Voting Tip #44
Be Patient – Wait for Official, Certified Results

Although we're all eager to know who the winners are in an election, voters need to be mindful that a complete, accurate count of all ballots cast in an election is a complicated process with many steps and multiple checks throughout the process to ensure not only an accurate vote count but compliance with all legal requirements.

With the expansion of methods (e.g., by mail and Early Voting – In person) plus the addition of steps to ensure voting opportunities for all (e.g., acceptance of military/overseas ballots received after Election Day and the utilization of the provisional ballot process), it will be many days after Election Day before all ballots are received, reviewed, and tabulated. Maryland, for example, counts any ballots postmarked on/before Election Day and received within ten (10) days after Election Day. Voters this November will need substantial patience for some results, as the deadline to complete the post Election Day tabulation procedures in California doesn't arrive until December 16th![42]

Why is so much time necessary? Election officials go through a painstaking set of steps to ensure that every valid vote counts and that no invalid one is included in the final tabulation. King County, Washington's Election Office describes the steps for tabulating ballots as follows.

[42] For a detailed list of the certification deadlines in force for the November 2022 General Election, see the National Conference of State Legislatures' "Canvass, Certification and Contested Election Deadlines and Voter Intent Laws," https://www.ncsl.org/research/elections-and-campaigns/after-the-voting-ends-the-steps-to-complete-an-election.aspx.

~ Copyright by Sharon Lawrence 89 ~

AMERICAN OVERSIGHT

Sorting the Incoming Ballot. Your ballot packet is returned to our office where a mail sorting machine scans the barcode for your information and takes a picture of the signature on the envelope. This signature will then be used in the verification process. You may watch ballot sorting live during an election.

Checking the Signature. State law requires that we compare your signature on the ballot envelope with your signature on file before we can count your ballot. If the signatures match, we can count your ballot. If the signatures do not match or is missing, we contact you by mail, email, and phone letting you know how to take care of the issue. You have until the day before the election is certified to respond. You may watch signature verification live during an election.

Opening the Ballot. Working with a batch of ballots, we first remove all the security envelopes from the return envelopes. This is the point where we separate the identity of the voter from the ballot inside the envelope to ensure your votes remain private. We then remove all ballots from the security envelopes.

Finally, we inspect the ballot to see if the votes as marked by the voter can be properly read by our scanning equipment. We flag ballots that need additional review and send all ballots to another workgroup to be scanned. You may watch ballot opening live during an election.

Scanning the Ballot. Once your ballot is ready for counting, we scan the ballots and store the images on a secure and closed system. The tabulation server is secured in a room with security cameras, biometric-controlled access, and tamper evident seals. You may watch ballot scanning live during an election.

Reviewing the Ballot. After ballots are scanned, we review the electronic images for any stray marks, unclear voter intent or corrections. We review ballots in teams of two people to ensure the votes are counted correctly. We use the **Voter Intent Manual**[43] created by the Office of the Secretary of State to ensure we are counting your votes as you intended. Using this guide ensures our voter intent decisions are made consistently from team to team and election to election. You may watch ballot review live during an election.

Counting Votes and Sharing Results. Tabulation occurs at 8 p.m. on Election Night and (unofficial) results are made public soon after. Scanning and counting continue daily until all eligible votes are counted and the election is certified.[44] You may watch ballot scanning live during an election.[45]

King County, Washington's elections staff produced an excellent set of short videos describing the vote county process:

---

[43] https://www.sos.wa.gov/_assets/elections/administrators/2018_voter-intent_web.pdf.

[44] Under the Revised Code Washington. Section 29A.60.190, county election officials have 21 days to certify the election.

[45] https://kingcounty.gov/depts/elections/how-to-vote/ballots/how-ballots-are-handled.aspx.

AMERICAN OVERSIGHT

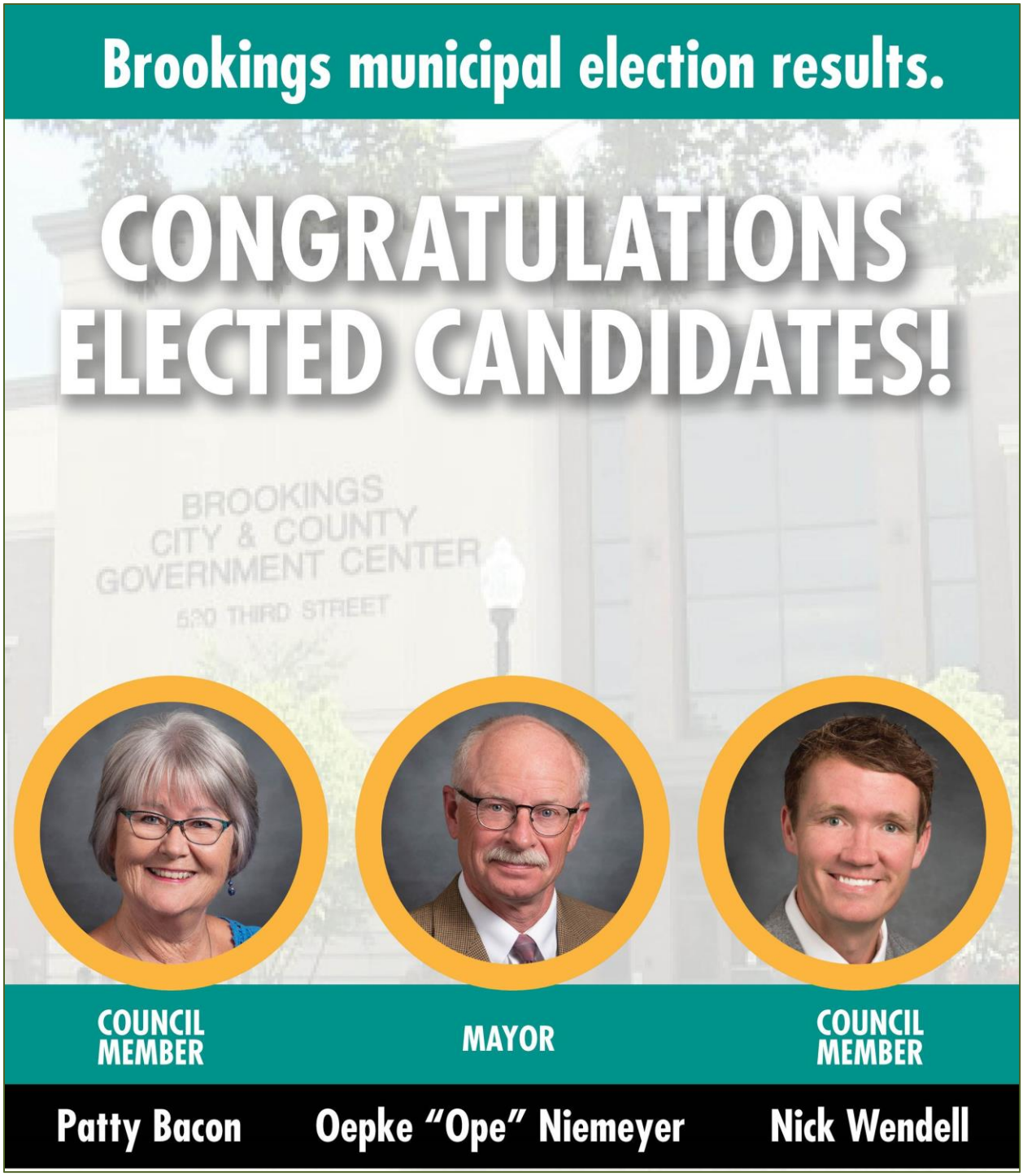
- ✦ Processing the Vote,[46]
- ✦ Counting the Vote, and[47]
- ✦ Certifying the Vote.[48]

The federal government's Election Assistance Commission offers a detailed overview of the election certification process and identifies "best practices" for election officials to use in tabulation of votes and certification of the results.[49]

[46] https://www.youtube.com/watch?v=6aZVW4mvi58&list=PLilCevjoKynIDNW2aWGaGYS8yB6xukVHT&index=1.
[47] https://www.youtube.com/watch?v=Vjq5FtQ8s7g&list=PLilCevjoKynIDNW2aWGaGYS8yB6xukVHT&index=2.
[48] https://www.youtube.com/watch?v=-dw4u3ykv9U&list=PLilCevjoKynIDNW2aWGaGYS8yB6xukVHT&index=3.
[49] https://www.eac.gov/election-officials/election-results-canvass-and-certification.

~ Copyright by Sharon Lawrence 91 ~

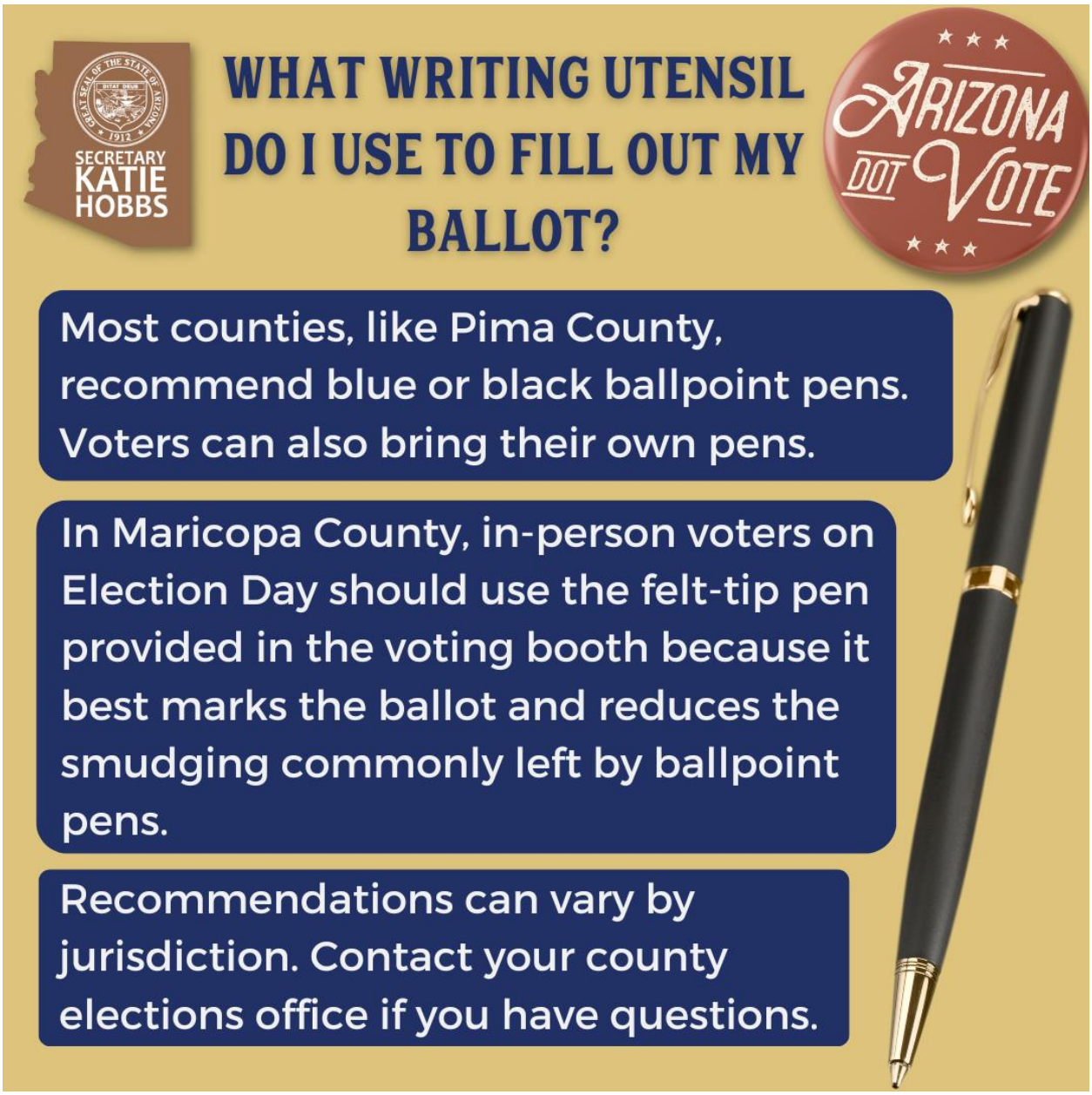
AMERICAN OVERSIGHT



Tip #45
Congratulate the Winners &
Accept the Certified Election Results!

~ Copyright by Sharon Lawrence 92 ~

AMERICAN OVERSIGHT



Appendix

~ Copyright by Sharon Lawrence 93 ~

AMERICAN OVERSIGHT

How Elections Work – The Basics

(Arizona Clean Elections Commission)

Arizona has a decentralized election system. What this means, is that there is not a single point of entry into our election system that could disrupt the entire process. Each county is responsible for conducting elections in their jurisdiction. For statewide elections, the counties conduct the election in their county and the Secretary of State aggregates the results from each county to determine the statewide results.

What are the key roles in Elections?. Arizona has 15 counties, and each county has a Board of Supervisors (elected positions), a County Recorder (elected position), and an Elections Director (appointed by the BOS or Recorder). While these entities are responsible for election administration, that administration must be done in accordance with election law.

The Arizona Legislature: The Arizona Legislature adopts laws related to the administration of elections. They set the policy for how elections should be conducted in the state of Arizona, including determining when elections are held, key deadlines such as when early voting begins and the qualifications for voting. Arizona Revised Statutes, Titles 16 and 19 apply to elections.

The Arizona Secretary of State: The Arizona Secretary of State (SOS) is the Chief Election Officer for the state. The Elections Services Division is responsible for certifying state election results, serves as the filing officer for federal, statewide and legislative candidates and statewide ballot measures. The SOS is responsible for the Elections Procedures Manual,[50] which details the procedures elections officials must follow to ensure election practices are consistent and efficient throughout the state. The SOS also certifies election equipment, conducts logic & accuracy tests on election equipment, administers Help America Vote Act (HAVA) funds, and maintains the statewide voter registration database.

The County Board of Supervisors: The Board of Supervisors (BOS) has specific election related responsibilities, including determining the polling places for Election Day, emergency early voting locations and certifying the official election results for the county. Importantly, the BOS also sets the budget for the County Recorder and County Elections Departments.

The County Recorder: The County Recorder is in charge of voter registration and early voting. The County Recorder's Office processes and maintains voter registration records, mails out early ballots and verifies early ballot affidavits and the voter signature. The County Recorder reviews and verifies every mail ballot to confirm the identity of the voter prior to the ballot being counted.

The County Election Director: The County Election Director is responsible for the conduct of elections on Election Day and ballot tabulation. The Election Director oversees the securing of polling places, hires and trains poll workers, conducts logic and accuracy testing on the equipment and tabulates the votes..[51]

---

50 https://azsos.gov/elections/arizona-election-laws-publications.

51 https://www.azcleanelections.gov.

~ Copyright by Sharon Lawrence 94 ~

AMERICAN OVERSIGHT



Photograph Courtesy of Maricopa County Elections Department

~~~~~~~~~~

Guidance on Polling Place Conduct & Preventing Voter Intimidation (Arizona)[52]

Free and fair elections are the foundation of our democracy, and Arizona's election officials are committed to ensuring all eligible Arizonans can exercise their right to vote. The Secretary of State's Office is providing the following guidance to:

(1) Educate voters, poll workers, observers, political parties, and other interested citizens about their respective roles, rights, and responsibilities and key polling place rules;
(2) Discourage unlawful voter intimidation and suppression; and
(3) Encourage voters to report suspected violations.

Reporting Voter Intimidation and Other Unlawful Conduct

If you witness voter intimidation or other unlawful conduct at the polls, we recommend the following steps:

First, inform a poll worker at the voting location, who will work to resolve any problems and call county election officials and/or local law enforcement if needed. However, if you or anyone else is in immediate danger, call 911 first and then inform a poll worker if possible.

52 https://azsos.gov/elections/about-elections/guidance-voting-location-conduct.

~ Copyright by Sharon Lawrence 95 ~

AMERICAN OVERSIGHT
~~~~~~~~~~

Document what you see as much as possible, including the who, what, when, and where of the incident. (But keep in mind that taking photos or video is prohibited inside the 75-foot limit of a voting location.)

You can also call 1-877-THE-VOTE. We will follow up with county election officials and federal, state, or local law enforcement entities if needed.

Make a Plan & Protect Your Vote

Know and plan ahead how, when, and where you will vote. Visit www.Arizona.Vote to find information about requesting a ballot-by-mail, voting early in-person, and voting on Election Day.

Rely on trusted sources for election information. In Arizona, your trusted sources are the Secretary of State's Office, County Recorders and Election Departments, and the Citizens Clean Elections Commission. Contact information is available at www.Arizona.Vote.

Report any misinformation about elections to the Secretary of State's Office at 1-877-THE-VOTE or elections@azsos.gov (link sends e-mail).

Persons Permitted Inside the 75-foot Limit of the Voting Location

Arizona law prescribes a 75-foot perimeter around each voting location to create a safe place to vote. Only the following persons are allowed inside the 75-foot-limit.

- ✦ Voters who are voting (may be accompanied by their children and/or someone to assist the voter);
- ✦ Election officials;
- ✦ Credentialed political party observers; and
- ✦ Authorized U.S. Department of Justice observers (for example, as required by court order).

The Role of Observers

All political party observers are required to obtain credentials from their county political party chairperson and must present those credentials at their assigned voting location to observe inside the 75-foot limit. Generally, only one observer per political party is permitted in each voting location.

Credentialed political party observers are there to do just that: observe. Observers shall not obstruct poll workers or the voting process, interact with voters, take videos or photos, act unprofessionally, or otherwise fail to obey the polling place inspector or rules established by the county. Party observers who violate these guidelines may have their credentials revoked by the county and be asked to leave.

Non-credentialed observers, interest groups, candidates, and members of the media are not allowed within the 75-foot limit. Even if you intend to observe outside the 75-foot limit, observers shall not obstruct voting lines or the entrance to the voting location, or otherwise engage in any conduct that may have the effect of threatening, harassing, or intimidating voters.

Activities Prohibited Inside the 75-Foot-Limit

To ensure a safe and secure voting experience for all Arizonans, the following activities are prohibited inside the 75-foot-limit of any voting location. If you experience prohibited activities in the 75-foot limit, inform a poll worker. Poll workers will generally be stationed inside the 75-foot limit. If you cannot find a poll worker, call the Secretary

~ Copyright by Sharon Lawrence 96 ~

AMERICAN OVERSIGHT

of State's Office at 1-877-THE-VOTE. We will use the information you provide to contact the appropriate county election officials to help resolve the issue.

Electioneering. It is unlawful to conduct campaign-related activity (electioneering) within the 75-foot limit. This includes handing out campaign literature, talking to voters or poll workers about candidates or issues, or otherwise attempting to influence the election. If the voting location has an "emergency" designation, electioneering is prohibited anywhere on-site, even outside the 75-foot limit.

A voter is permitted to wear clothing with a political message inside the 75-foot limit, but poll workers, observers, and election officials may not.

Carrying Firearms and Weapons. Arizona law prohibits private citizens, even if properly licensed, from entering the 75-foot limit of a voting location with a weapon. Further, since many polling places are located in schools, it may be unlawful to bring a firearm on school property, even outside the 75-foot-limit.

Openly carrying a firearm outside the 75-foot limit is also problematic and likely to result in unlawful voter intimidation. Additionally, any aggressive or ostentatious display of a weapon will almost certainly constitute an act of intimidation.

Arizona's election officials seek to ensure voting locations are not only safe, but also free of intimidation. If you are coming to a voting location for any reason, please leave any weapons at home or in your vehicle.

Taking Photographs and Videos. While taking photos of your early ballot from home ("ballot selfies") is permissible, taking any photos or videos in a voting location inside the 75-foot limit is prohibited and punishable as a misdemeanor.

Further, much like the open display of firearms, taking photos or videos outside the 75-foot-limit may have an intimidating effect on voters entering or exiting the voting location if done in an aggressive, threatening, or harassing way. Filming voters based on race, ethnicity, religion, or political affiliation is inappropriate.

If you find it necessary to film to document the commission of a crime or other election-related violation, please consider informing a poll worker first.

Law Enforcement and Uniformed Personnel

Generally, law enforcement officers, whether uniformed or plain-clothes, should not be stationed within the 75-foot limit of a voting location. Exceptions may apply if the officer is voting, if the voting location is located within a public safety building, or if an officer is called to respond to a specific emergency.

The presence of uniformed law enforcement personnel at a voting location, whether in or outside of the 75-foot limit, may have the effect of intimidating voters. Counties will balance this potentially intimidating effect with the need to preserve the peace and respond to emergencies.

As noted below, each voting location is overseen by an inspector and has a designated election marshal charged with keeping order in and around the voting location. Poll workers should make all reasonable efforts to de-escalate disturbances without engaging law enforcement whenever possible. Situations that cannot be solved by poll workers should be resolved with the assistance of county election officials. In circumstances where there is violence or threats of violence, including any instance when a private citizen carries a weapon into the 75-foot limit, the marshal or election officials should contact law enforcement for the limited purpose of resolving that situation.

~ Copyright by Sharon Lawrence 97 ~

AMERICAN OVERSIGHT

Voter Challenges

All eligible voters are entitled to exercise their right to vote free from harassment and intimidation from baseless challenges to voter qualifications. Arizona law permits only a qualified elector of the county to challenge a voter's eligibility to vote, and political party challengers must be previously designated and credentialed as observers by their party.

A qualified elector challenging a voter's eligibility must have clear and convincing evidence that:

- The voter has voted before in that election;
- The voter is not the person whose name appears in the roster/e-pollbook;
- The voter has not resided in Arizona (or the relevant locality) for at least 29 days before the election;
- The voter is registered at an address that is not permitted for registration purposes; or
- The voter is not otherwise a qualified elector, for example, the voter does not live within the proper electoral district or is not at least 18 years old.

Challenges must be directed to poll workers, and challengers shall not directly confront voters or question voters about their voting qualifications. Challenges must be promptly decided in the voting location by a board made up of the inspector and two judges, pursuant to applicable law and the Elections Procedures Manual.

- The voter must be permitted to vote a regular ballot if: (1) the voter appears to be registered and takes the prescribed oath, or (2) a majority of the board finds the challenge invalid.
- The voter must be permitted to vote a provisional ballot if: (1) the voter refuses to take any oath; (2) the voter refuses to answer the inspector's questions material to the challenge; or (3) a majority of the board finds the challenge is valid.

Critically, challenges based in whole or in part on race, national origin, appearance, surname, language, or religion are not permitted, and violate federal anti-discrimination laws. Repeated challenges without a sound basis that delay voting, challenges that are otherwise intended to intimidate or prohibit qualified voters from voting, or challenges that involve additional confrontational or harassing behavior may amount to unlawful voter harassment and intimidation and warrant removal from the voting location.

Dropping off Ballots at Voting Locations

All eligible voters may request a ballot-by-mail and may mail back their voted ballot or drop it off at their County Recorder's Office, any official ballot drop-box, any early voting location, or any Election Day voting location in the county. Ballots must be received by election officials by 7:00 p.m. on Election Day.

Arizona law allows a caregiver, family member, household member, or election official to help return a voter's ballot to county election officials, including dropping off the ballot at a voting location. These categories are broadly defined:

- A caregiver is a person who provides medical or health care assistance to the voter in a residence, nursing care institution, hospice facility, assisted living center, assisted living facility, assisted living home, residential care institution, adult day health care facility or adult foster care home."
- Family member: "a person who is related to the voter by blood, marriage, adoption or legal guardianship."
- Household member: "a person who resides at the same residence as the voter."

~ Copyright by Sharon Lawrence 98 ~

AMERICAN OVERSIGHT

Discriminatory Conduct and Voter Intimidation

Discrimination against voters based on race, ethnicity, national origin, language, religion, or disability is punishable under law. Even in the absence of discrimination, any attempt to intimidate, coerce, or threaten a person to vote or not vote is strictly prohibited and may be criminally punishable.

Examples of activity that may amount to intimidation, whether in or outside the 75-foot limit, include:

- ✦ Aggressive or ostentatious display of weapons;
- ✦ Aggressive behavior, such as raising one's voice or taunting a voter or poll worker;
- ✦ Using threatening, insulting, or offensive language to a voter or poll worker;
- ✦ Blocking the entrance to a voting location or disrupting voting lines;
- ✦ Intentionally disseminating false or misleading information at a voting location, such as flyers or communications that misstate the date of the election, hours of operation for voting locations, addresses for voting locations, or similar efforts intended to disenfranchise voters;
- ✦ Impersonating a law enforcement officer, or otherwise wearing clothing, uniforms or official-looking apparel, intended to deter, intimidate, or harass voters (see also A.R.S. § 26-170, prohibiting unauthorized wearing of national guard or U.S. armed forces uniform);
- ✦ Directly confronting or questioning voters in a harassing or intimidating manner, including asking voters for "documentation" or other questions that only poll workers should perform;
- ✦ Raising repeated frivolous voter challenges to poll workers without any good faith basis, or raising voter challenges solely based on race, ethnicity, national origin, language, religion or disability; or
- ✦ Posting signs or communicating messages about penalties for "voter fraud" in a harassing or intimidating manner.

In sum, any activity that has the intent or effect of threatening, harassing, or intimidating voters—whether in or outside of the 75-foot-limit—is unlawful and should be strictly enforced by election officials, including with assistance from law enforcement if necessary.

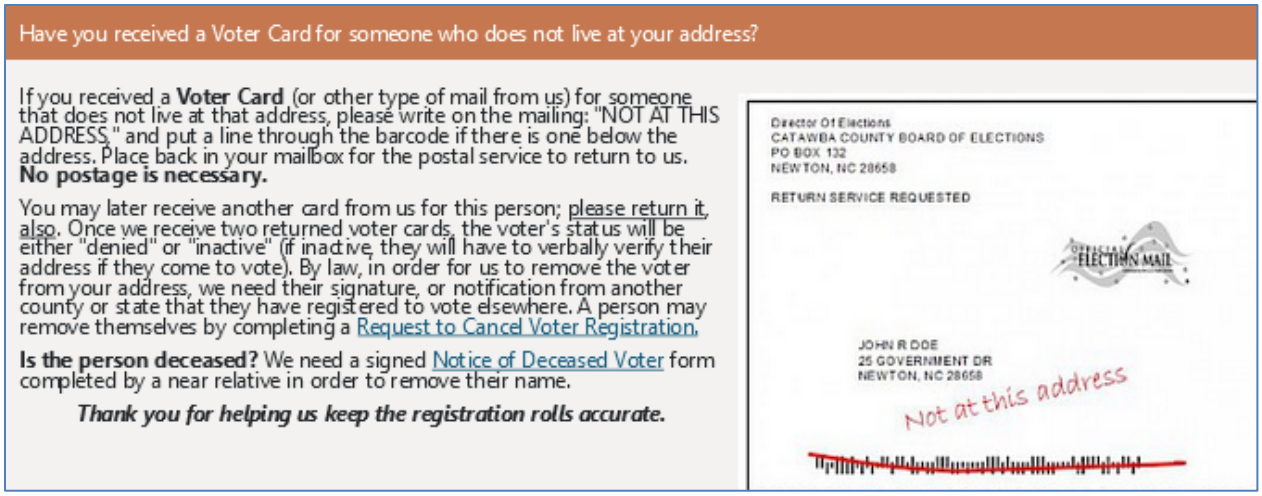
Enforcing Polling Place Rules

Inspectors oversee each polling place and should utilize the marshal to preserve order and remove potentially disruptive persons. Higher-level decisions generally are raised through county channels, whether through a trained troubleshooter, the elections department, or both. Any decision to contact law enforcement is for local election officials to be exercised in their sound judgment.

If you witness a problem at a polling place, you should not speak to or accost a voter to "enforce" the law yourself. Tense situations should be de-escalated, not escalated. Please inform a poll worker to resolve the issue, or if you or another person is in immediate danger, call 911. Do not take matters into your own hands.

~ Copyright by Sharon Lawrence 99 ~

AMERICAN OVERSIGHT



Techniques and Tools to Ensure Election Security

Safeguards Against Vote Fraud

Deterring Double Voting. Many people may believe that an easy way to commit election fraud is to vote in multiple states (e.g., all states where the potential voter owns property). Beyond the fact that election laws are designed to ensure that each individual has only one official residence for voting purposes, election officials are using modern technology to uncover double voting.

Thirty-three (33) states and the District of Columbia now participate in the Electronic Registration Information Center (ERIC)[53] which compares data from participating states to voters that could/might be voting simultaneously in multiple locations. Data about potentially problematic voters are transmitted to the involved states for further investigation and possible removal from the rolls and/or criminal prosecution,

For a detailed look at how voter registration lists are scrubbed of unqualified voters, see the following article for an explanation of the process used by the State of Michigan. See also the sample above of one of the methods that Catawba County, North Carolina election officials use to promote accuracy in their voter rolls.

Preventing the Exertion of Undue Influence on the Elderly. Although election fraud is extremely rare, one area of concern has been the vulnerability of elderly individuals living in group settings to undue influence from facility staff or outsiders. A number of states address the vulnerability, while also facilitating active participation by the residents in the election process.

Under Rhode Island General Law 12-20-14, any mail ballot requested from residents of hospitals, convalescent homes, nursing homes, rest homes or similar institutions (public or private) within the state must be administered by a bi-partisan team of election officials from the Board of Elections. These teams are called Nursing Home Supervisors. They are charged with the responsibility to:

- ✦ Pick up ballots assigned to voters;
- ✦ Make appointments with Activities Directors at in-state nursing homes;
- ✦ Deliver ballots to voters on an assigned day;
- ✦ Work in teams to assist the voter with marking his/her ballot (including marking the ballot for the voter at his/her direction); and

53 https://ericstates.org.

~ Copyright by Sharon Lawrence 100 ~

AMERICAN OVERSIGHT

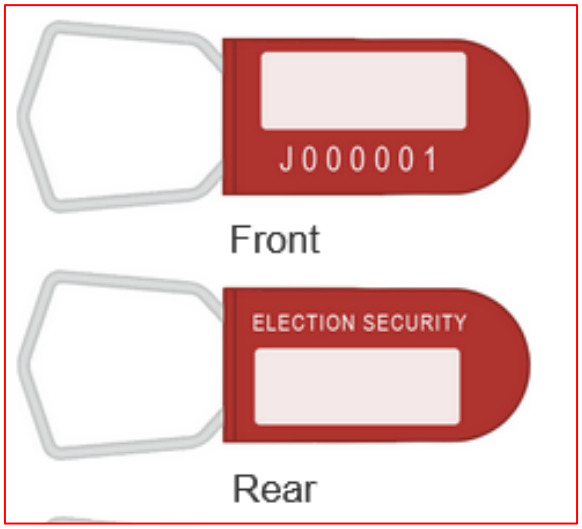
- ✦ Witness ballots and transport to the Board of Elections for tabulation;

Catawba County, North Carolina election officials take a similar approach. They utilize a Multi-partisan Assistance Team (MAT) to visit adult care homes, hospitals, nursing homes, and similar facilities at election time to assist residents in voting, as needed. Appointed by the County Board of Elections, each team consists of at least two members who are either of different political parties and/or unaffiliated.[54]

Safeguards Against Tampering with Election Materials or Equipment

Equipment Security. Like many jurisdictions, Delaware County, PA has a staff whose sole job is to manage/protect the voting equipment. Here's a brief summary of that Department's responsibilities.

> **VOTING MACHINES DEPARTMENT**
>
> The Voting Machine Department is responsible for the storage, security, programming, testing, and delivery of all voting equipment and precinct supplies for the 428 Delaware County precincts, which are housed in more than 300 polling locations on Election Day. All potential changes in polling place locations are inspected to ensure polling place guidelines and compliance with the standards under the Americans with Disabilities Act (ADA).
>
> The Chief Custodian manages a call center on Election Day and dispatches roving technicians in different sectors of the County to check on precincts and/or to trouble-shoot voting equipment issues, replace any equipment or supplies and deliver any supplemental materials that might be needed on Election Day.
>
> The official post-election Review Board process is conducted at the Voting Machine Warehouse overseen by the Chief Custodian of the Voting Machine Department. The Voting Machine Warehouse also retrieves, inventories and re-stocks voting equipment and election supplies between Elections. [55]



The equipment won't be secured only in the warehouse. Every machine or storage/transport device will have a tamper-evident seal of some type (with serial number) to enhance the other security features (e.g., being stored in an alarmed/locked warehouse.) (See illustration to the left) Serial numbers for all items are, of course, meticulously reordered and tracked.[56]

Video Surveillance. In many jurisdictions, live video surveillance is fast becoming the norm. Texas law now requires all counties of 100,000 population or more "to establish a video recording system that captures all areas containing voted ballots from the time that the ballots are delivered to the central counting station (CCS), early voting ballot board (EVBB), or signature verification committee (SVC) until the local canvass of election results. The video recording must also be made available as a livestream during that timeframe."[57] Texas law further provides:

---

54 https://catawbacountync.gov/site/assets/files/2333/mat_flyer.pdf.
55 https://www.nhpr.org/2022-09-06/barnstables-ballots-stuck-in-the-vault-voting-on-hold.
56 See https://lnkd.in/gnG3MwPT for more samples.
57 Section 127.1232(b) of the Election Code.

~ Copyright by Sharon Lawrence 101 ~

AMERICAN OVERSIGHT

> If the voted ballots will be moving from one location to another location during the required timeframe, the recording should also record those voted ballots while they are in transit through hallways or other areas in the office. The general custodian may use either a moving camera to follow the ballots while they are in transit or may set up stationary cameras throughout the hallways to capture the areas where those ballots will be travelling. If there are limitations in recording capabilities while in transit, the general custodian should allow poll watchers, if feasible, to accompany or witness the transfer process.

To assure all interested parties of the security of the elections process, elections officials in Ada County, Idaho allow Internet access to the live feed from the video camera trained on their absentee ballot cage and 12 other areas.[58]

Ballot Drop Box (BDB) Security. Clinton Township, Michigan, equips each of their six boxes with four surveillance cameras. According to recent news articles, the elections administrator may view a live stream from each of the boxes on her cell phone. "The cameras capture the voter as they arrive, and another camera captures the license plate as they leave. There's also a camera inside the drop box which can capture the voters face and how many ballots they put in. Another camera behind the drop box makes sure no one tampers with it."[59] (Note: Four of the six are located at fire or police stations.)[60]

Yolo County, California election officials explain the process they use to ensure the security of ballots deposited in their boxes.

- ✦ Two (2) Yolo County Ballot Drop Box Retrieval Team member collect the ballots from the official BDBs on a mandated schedule using a documented chain-of-custody procedure.
- ✦ Vote by Mail ballots collected from the BDBs go through the same signature verification procedures as ballots returned by mail.
- ✦ On Election Day, BDB Retrieval Teams will be at all BDB locations to secure the BDB at the close of the polls at 8 p.m.

Any voter waiting in line to deposit a Vote By Mail ballot will be able to drop off their ballot.

Systems in Place to Ensure Accurate Tabulation of Votes

Checks and Rechecks Throughout the Voting Process. Wisconsin provides an excellent short summary of the state mandated security procedures which must be followed throughout the election process.

> **Public Test of Voting Equipment.** All municipalities are required to conduct a public test of their voting equipment within 10 days of each election. Pre-election testing is intended to confirm the accuracy of voting equipment programming. This event is considered a public meeting and must be noticed at least 48 hours prior. The public is invited to attend and observe the testing process.
>
> Programming is verified by feeding a set of pre-marked ballots into each machine and reviewing the results tape that is generated. Vote totals for each candidate in a contest should differ so that any errors in a contest can be detected. An errorless count is required at the conclusion of the process. Any anomalies identified in testing must be remedied before the equipment can be used in an election.
>
> **Post Public Test and Election Day Security Procedures.** Following the public test, the voting equipment and memory devices are required to be secured. The memory device must remain in the equipment with a tamper-evident seal used to secure memory device compartments. A chain-of-

---

58 https://adacounty.id.gov/elections/ballot-cameras.

59 See this article, which also includes video from one of the cameras, https://www.wxyz.com/news/democracy-2022/clinton-township-installs-new-upgraded-security-cameras-at-ballot-drop-boxes (October 13, 2022).

60 https://clintontownship.com/184/Elections.

AMERICAN OVERSIGHT

custody log is required to be maintained that documents any access to each memory device or tabulator. Verification of the serial numbers must take place before the polls open in the morning and after the close of polls. The Wisconsin Elections Commission (WEC) also recommends that election officials verify this information throughout Election Day. All access to the memory device must be documented on the Inspectors' Statement.

Post-Election Audit of Voting Equipment. Wisconsin statutes require a post-election audit of voting systems used in Wisconsin after each General Election. The audit is designed to assess the accuracy and performance of each voting system approved for use in the state. The audit is a public meeting and proper notice must be provided at least 48 hours in advance. A representative sample of reporting units that use each type of voting equipment are included in the selection process. The parameters of each audit are established by the Elections Commission.

During this process, elections workers conduct an independent hand count of paper ballots and tally the results of the contests. The final hand-count tally total is compared to the election night voting system results. Audit materials are submitted to WEC for review. Any discrepancies are investigated by WEC staff. Commission staff may request a vendor investigate and provide explanation for any unexplained discrepancies. WEC may, at its sole discretion, choose to re-test any voting system should unexplainable issues arise in the audit.[61]

Certification of the Election Results. Once the ballots are cast, a detailed process is set in motion to ensure the integrity of the elections leading to certification of the results. Here's how the process works in Minnesota.

Election results are not official until they have been reviewed and certified by a canvassing board. If necessary, the canvassing board oversees a recount. Canvassing boards are also involved in the process of randomly selecting precincts for review after every election.

Unofficial Results. On Election Night, county election officials enter unofficial election results on the Office of the Secretary of State's website. Following Election Day, county election officials audit and proof their work to make any corrections as necessary before they canvass their results. It is routine for election officials to discover a number of small errors or typos, such as transposition of digits (e.g., entering the number 48 instead of 84).

County Canvassing Board. Once results have been proofed by county election officials, the county canvassing board must review and approve the results before they are official. A county canvassing board certifies the votes cast within the county for races that go beyond the county boundaries and certifies the election results for offices up for election that are voted upon exclusively within that county (county offices and legislative districts that are entirely contained within the county). Federal offices, statewide offices, and legislative districts that cross county lines must be certified by the state canvassing board.

Every county establishes a county canvassing board of five members: the county auditor; the court administrator of the district court in that county; the mayor or chair of the town board of the most populous municipality in the county; and two members of the county board. Each municipality and school district has its own canvassing board to certify results in those races.

The county canvass report is sent to the Office of the Secretary of State where it is carefully reviewed and incorporated into a statewide canvass report that is presented to the State Canvassing Board.

State Canvassing Board. The state canvassing board, like a county canvassing board, meets following each state primary and general election. It meets at the secretary of state's office seven days following a state primary election and on the third Tuesday following a state general election.

---

61 https://elections.wi.gov/elections/voting-equipment-wisconsin/voting-equipment-security.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 103 ~

> The state canvassing board is responsible for canvassing and certifying the results of all statewide elections, including state and federal offices, state constitutional amendment ballot questions, and state legislative and judicial offices that overlap more than one county. In conducting the canvass, the state canvassing board compiles and reviews the results as indicated by each of the 87 county canvassing reports. If necessary, upon the request of an apparent losing candidate, the state canvassing board oversees a recount of the results for that office.
>
> The state canvassing board is made up of five members. The Secretary of State serves as chair. To fill out the board, the secretary appoints two members of the State Supreme Court and two judges from a district court.[62]

Recounts. Some states mandate an automatic recount (at government expense) if the last tabulation of the votes puts the top two candidates within a certain percentage (e.g., less than ½ of 1 percent). In other cases, recounts will move forward if a losing candidate calls for a recount and pays for the cost of that effort. Minnesota law, for example, declares:

> **Publicly Funded Recounts.** A publicly funded recount for a federal office, state constitutional office, or judicial office may occur if the difference in the number of votes cast for the apparent winning candidate and any other candidate is less than one-quarter of 1 percent (0.25 percent).
>
> A publicly funded recount of the results of an election for a state legislative office may occur if the difference in the number of votes cast for the apparent winning candidate and any other candidate is less than one-half of 1 percent (0.5 percent).
>
> A publicly funded recount may also occur in any race where the difference in votes cast is ten votes or less and the total number of votes cast for the office is 400 or fewer.
>
> A publicly funded recount will occur if the apparent losing candidate requests one by filing a notice with the appropriate filing officer within 48 hours after the canvassing board meeting.
>
> **Discretionary Recounts.** A discretionary recount of the results of an election for federal office, state constitutional office, legislative office, or judicial office can occur at the candidate's expense if the difference in the number of votes cast for the apparent winning candidate and any other candidate is greater than the threshold for a publicly funded recount. An apparent losing candidate must submit a request for a discretionary recount along with the funds to cover the cost of the recount within five days of the canvass of a primary election or within seven days of the canvass of a general election.
>
> A candidate who requests a discretionary recount may specify up to three precincts to be recounted first; the candidate may waive the remainder of the recount after the specified precincts are recounted.
>
> **Recounts of Ballot Questions.** Recounts of ballot questions follow a similar process as that described above, except that any recount must be requested through a petition process.[63]

Virginia's State Board of Elections outlines its elaborate instructions for a recount in its **Virginia Election Recounts: Step-by-Step Instructions.** [64]

---

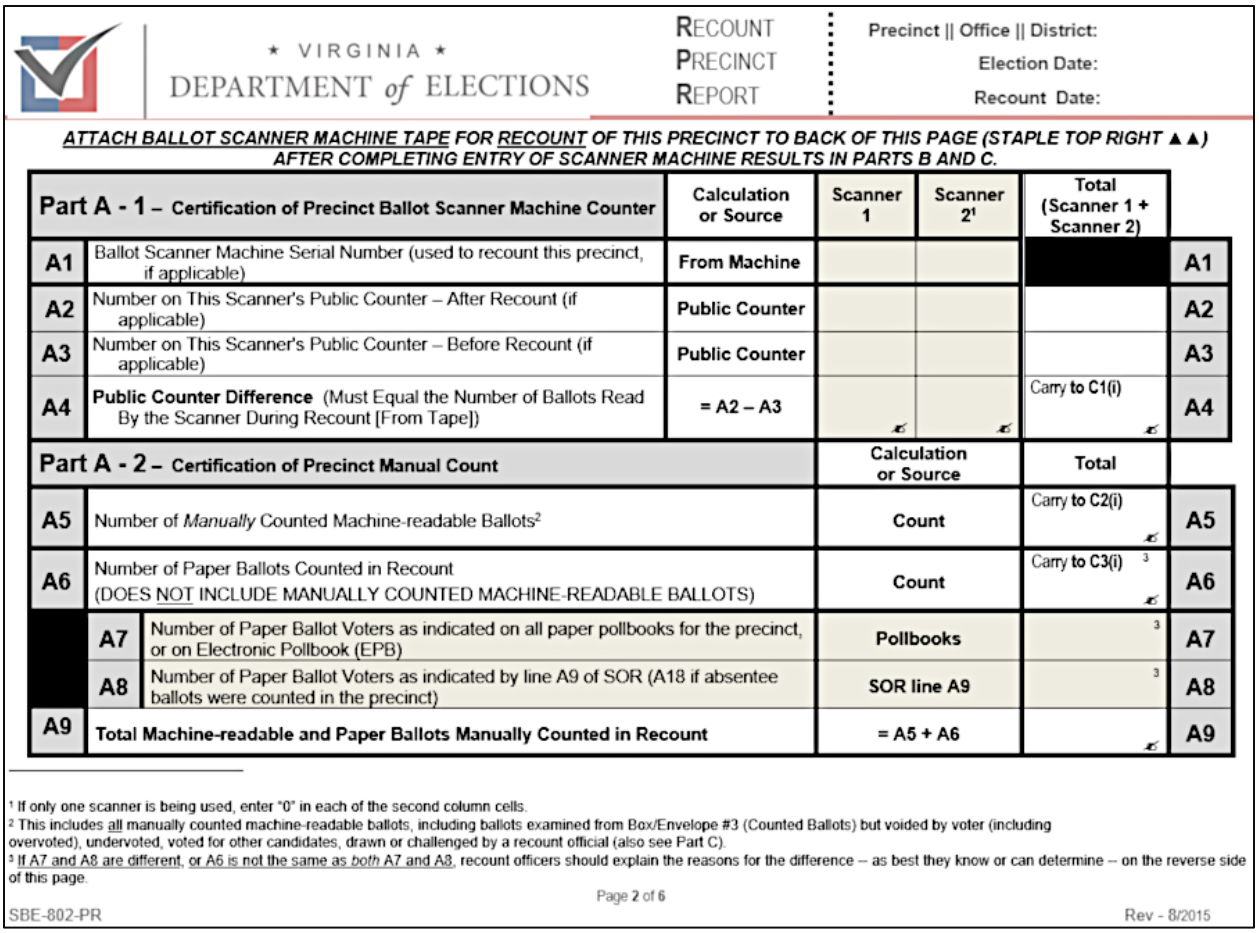
62 https://www.sos.state.mn.us/elections-voting/how-elections-work/canvassing-boards/.

63 https://www.sos.state.mn.us/elections-voting/how-elections-work/recounts/#:

64 https://www.elections.virginia.gov/media/formswarehouse/recount/officials/Recount-Step-by-Step-2015.pdf.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 104 ~



★ VIRGINIA ★
DEPARTMENT of ELECTIONS

RECOUNT PRECINCT REPORT

Precinct || Office || District:
Election Date:
Recount Date:

ATTACH BALLOT SCANNER MACHINE TAPE FOR RECOUNT OF THIS PRECINCT TO BACK OF THIS PAGE (STAPLE TOP RIGHT ▲▲)
AFTER COMPLETING ENTRY OF SCANNER MACHINE RESULTS IN PARTS B AND C.

Part A - 1 – Certification of Precinct Ballot Scanner Machine Counter		**Calculation or Source**	**Scanner 1**	**Scanner 2[1]**	**Total (Scanner 1 + Scanner 2)**	
A1	Ballot Scanner Machine Serial Number (used to recount this precinct, if applicable)	**From Machine**				A1
A2	Number on This Scanner's Public Counter – After Recount (if applicable)	**Public Counter**				A2
A3	Number on This Scanner's Public Counter – Before Recount (if applicable)	**Public Counter**				A3
A4	**Public Counter Difference** (Must Equal the Number of Ballots Read By the Scanner During Recount [From Tape])	**= A2 – A3**			Carry to C1(i)	A4
Part A - 2 – Certification of Precinct Manual Count			**Calculation or Source**		**Total**	
A5	Number of *Manually* Counted Machine-readable Ballots[2]		**Count**		Carry to C2(i)	A5
A6	Number of Paper Ballots Counted in Recount (DOES NOT INCLUDE MANUALLY COUNTED MACHINE-READABLE BALLOTS)		**Count**		Carry to C3(i) [3]	A6
A7	Number of Paper Ballot Voters as indicated on all paper pollbooks for the precinct, or on Electronic Pollbook (EPB)		**Pollbooks**		[3]	A7
A8	Number of Paper Ballot Voters as indicated by line A9 of SOR (A18 if absentee ballots were counted in the precinct)		**SOR line A9**		[3]	A8
A9	**Total Machine-readable and Paper Ballots Manually Counted in Recount**		**= A5 + A6**			A9

[1] If only one scanner is being used, enter "0" in each of the second column cells.
[2] This includes all manually counted machine-readable ballots, including ballots examined from Box/Envelope #3 (Counted Ballots) but voided by voter (including overvoted), undervoted, voted for other candidates, drawn or challenged by a recount official (also see Part C).
[3] If A7 and A8 are different, or A6 is not the same as *both* A7 and A8, recount officers should explain the reasons for the difference -- as best they know or can determine -- on the reverse side of this page.

Page 2 of 6

SBE-802-PR Rev - 8/2015

Transparency

Mindful of the concerns that community members had about the elections process, Boulder County, Colorado election officials enhanced their election security strategy by adding an Election Security Community Briefing to the process. Officials explained:

> Our office has prioritized security throughout all of our operations, conducting formal assessments and implementing steps to protect and affirm our most sacred right as Americans. We know that we have a central role to play in sustaining your trust in our elections, so we are continually enhancing our security posture by adopting advanced security procedures, technologies, and innovations that protect the sanctity of votes and voter information. We have also implemented significant staff security awareness training and forged stronger partnerships with local, state, and national entities.
>
> Our office also believes that our work to enhance election security will be most effective when the voting public understands it: meaningful transparency strengthens our democracy. We must communicate what we are doing so our community can have a deep understanding of what the threats are, how we are actively working to mitigate them, and how they can partner with us in these efforts. That is why we created this Boulder County Elections – Election Security Community Briefing. Our goal with this report is to ensure our community understands Boulder County's approach to election security and the actions we are undertaking to protect your voter information and the integrity of your vote.[65]

65 https://assets.bouldercounty.gov/wp-content/uploads/2020/09/BoulderCountyElections-Election-Security-Community-Briefing.pdf.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 105 ~

Indiana Election Division
Election Security Overview[66]

In Indiana, we take great care to prepare for each election. The security of our election systems is of the utmost importance, and in addition, to physical and cyber security, information is a powerful defense. In partnership with counties, other states, and the federal government, we are developing new answers to security concerns and election policy. Some of the tools and precautions being taken in Indiana to ensure secure voting include:

Our Partners

Voting System Technical Oversight Program (VSTOP). Hosted by Ball State University, this program tests all of the election equipment used in Indiana for an added layer of safety and security. After VSTOP reviews the system to ensure its compliance with the law, their recommendation is presented to the bi-partisan Indiana Election Commission, the body responsible for certifying voting systems for use in Indiana.

IU Center for Applied Cybersecurity Research (CACR). The Indiana Secretary of State's Office has partnered with Indiana University to review and improve the state's election cybersecurity incident response plan and will help prepare election officials in all 92 Indiana counties for cybersecurity incidents related to the 2020 General Election and beyond. The project will have three parts:

- ✦ Creation and delivery of a suite of materials and table-top training events prior to the 2020 elections, including a series of regional "boot camps" with county clerk offices to train election officials about how to respond to different forms of cyberattacks, such as phishing, phone scams, and impersonation calls.
- ✦ Ongoing consulting with Indiana's Secretary of State and county clerks during the 2020 election season
- ✦ Post-election documentation of lessons learned and recommendations for the future

FireEye. FireEye provides intrusion detection and prevention systems at the state and county level. They monitor internet traffic accessing websites and databases to prevent bad actors from accessing critical election information. This partnership not only prevents and blocks cyber threat, in the event of an incident, FireEye will provide resources to remove the threat.

Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). An independent entity that partners with the U.S. Department of Homeland Security, this allows us access to 24/7 security information, threat notifications, and security advisories.

U.S. Department of Homeland Security. The Federal Government has conducted risk and vulnerability testing to secure Indiana's electronic information such as the Statewide Voter Registration System and the state election website.

Our Tools

Multifactor Authentication Protocol for County Election Offices. The Statewide Voter Registration System is used by the state and the counties to maintain voter registration list. We are investing in security at all levels by implementing validation requirements to ensure only authorized users can access the system.

Multifactor Authentication Protocol for all Voters. Hoosiers utilize IndianaVoters.com to register to vote, update their voter information, find their polling location and much more. The state is investing in security at all levels by implementing validation requirements to enhance security for public online access of voter registration information on indianavoters.com, if the voter chooses to do so.

---

66 https://indianavoters.in.gov/MVPHome/ElectionSecurity

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 106 ~

Voter Verifiable Paper Audit Trail. A voter verifiable paper audit trail (VVPAT) is a security measure that allows voters to independently verify their vote was correctly recorded. Further, Indiana law allows for county election boards to select the voting equipment used in their counties, as long as those systems are certified for use in Indiana.

Currently, state law allows for the use of an optical scan ballot card system (OpScan) or direct record electronic system (DRE). OpScan voting systems employ a voter verifiable paper audit trail (VVPAT) by nature of its design – using ballot card marked by the voter or a ballot marking device that is then tabulated by an optical scan component. All DRE systems must contain a VVPAT component not later than July 1, 2024.

Penetration Testing. Penetration testing, also called ethical hacking, is a practice of testing a computer system, network, or web applications to find security vulnerabilities that could be exploited. The State periodically conducts penetration testing to identify potential security vulnerabilities. Once vulnerabilities have been identified steps will be taken to address identified security vulnerabilities and strengthen the security of the Indiana elections infrastructure.

Cloudflare. Distributed denial of service attacks known as DDOS attacks are used to take down websites. To prevent this, the State has implemented a distributed denial of service content filter called Cloudflare to protect indianavoters.com.

Cyber Best Practice Training. Each year the Voting System Technical Oversight Program (VSTOP) team provides Indiana counties with best practices for the operation of election equipment and cybersecurity. Best practices are updated each year as cyber threats evolve and the election landscape changes.

Risk Limiting Audits. A risk limiting audit (RLA) is a post-election audit of ballots. A RLA requires manually reviewing a sample of ballot cards of a VVPAT component to a DRE to ensure election results are interpreted and tallied correctly.

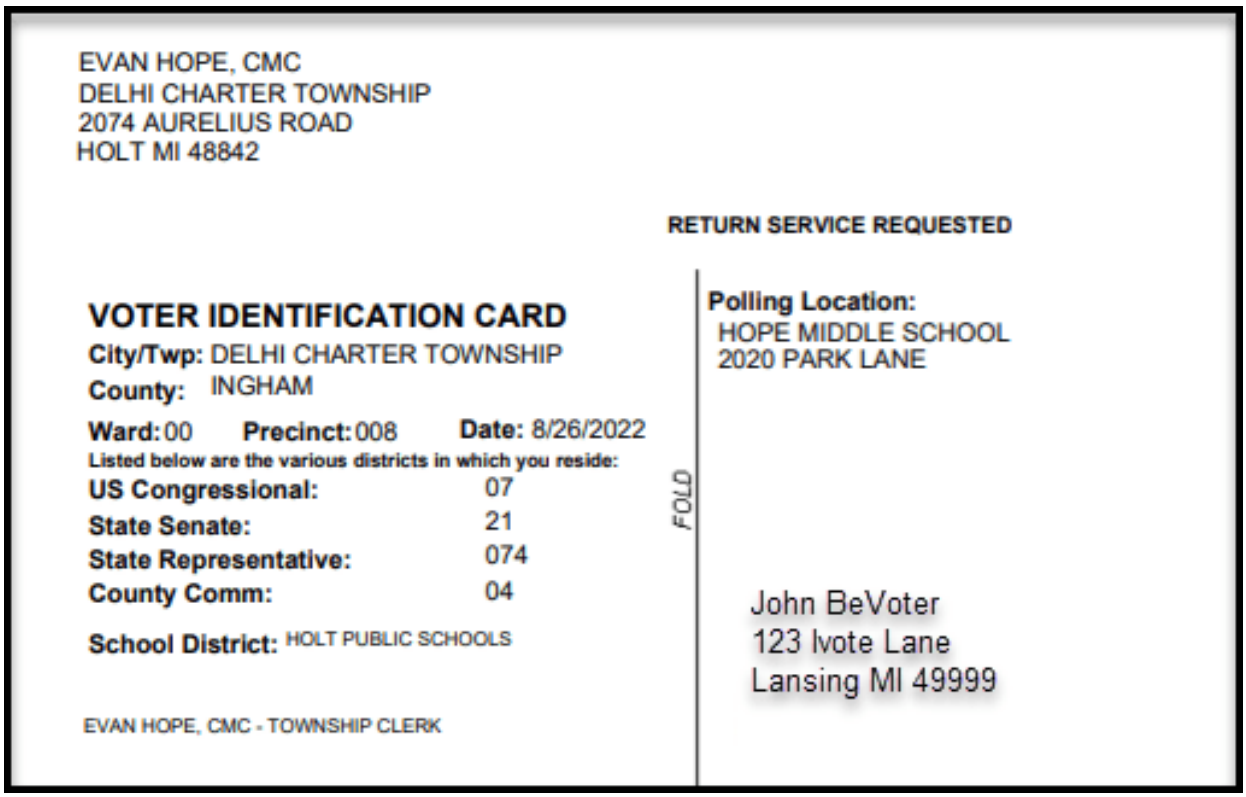
Security Protocol. State law establishes physical security standards for election equipment. Many county election boards adopt customized security resolutions above and beyond what is required by law.

It's also important to know that no piece of Indiana's voting equipment is online. The machines and tabulators are not connected to the internet. Public tests of voting systems are conducted in all counties prior to an election, and are open to the public. If you would like to attend, contact your county administrators for times and locations.

We take the security of our elections process very seriously and are working diligently to ensure that every available defense is utilized. Indiana has taken many steps to secure our elections, but let's be clear: there will always be new recommendations, new technology, and new best practices where cybersecurity is concerned. The way we administer elections must continue to evolve, because this is a race without a finish line. We are fully committed to ensuring that we continue to move forward, using every tool at our disposal to maintain safe and secure voting for all Hoosiers.

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 107 ~



EVAN HOPE, CMC
DELHI CHARTER TOWNSHIP
2074 AURELIUS ROAD
HOLT MI 48842

RETURN SERVICE REQUESTED

VOTER IDENTIFICATION CARD

City/Twp: DELHI CHARTER TOWNSHIP
County: INGHAM

Ward: 00 **Precinct:** 008 **Date:** 8/26/2022

Listed below are the various districts in which you reside:

US Congressional:	07
State Senate:	21
State Representative:	074
County Comm:	04

School District: HOLT PUBLIC SCHOOLS

EVAN HOPE, CMC - TOWNSHIP CLERK

FOLD

Polling Location:
HOPE MIDDLE SCHOOL
2020 PARK LANE

John BeVoter
123 Ivote Lane
Lansing MI 49999

Voter Registration Cancellation Procedures (Michigan)[67]

How Voter Rolls are Maintained in Michigan

Michigan's list of registered voters is maintained on the Qualified Voter File, a database developed by the state of Michigan and maintained by municipal and county clerks and the Bureau of Elections. The Qualified Voter File contains the names of all individuals registered to vote in Michigan. It also contains the names of individuals with cancelled registrations, who are no longer eligible to vote in Michigan. The Qualified Voter File is constantly updated whenever a new voter registers, a voter updates his or her registration information (such as an address), or a voter's registration is cancelled.

Voter registrations are cancelled primarily for one of four reasons:

- A voter moves away from their voting jurisdiction.
- A voter dies.
- A voter registration is identified as a duplicate.
- A voter requests that his or her registration be cancelled.

Local and state election officials use a variety of methods to identify voters whose address changes.

- As part of the Michigan's automatic voter registration law, when a registered voter updates his or her driver's license or state ID address, the voter's registration is also updated. If a voter moves within his or her city or township, the registration moves to the voter's new

[67] https://www.michigan.gov/sos/elections/upcoming-election-information/voters/voter-registration-cancellation-procedures.

~ Copyright by Sharon Lawrence 108 ~

AMERICAN OVERSIGHT

address. If a voter moves to a different city or township in Michigan, the voter's previous registration is cancelled, and the voter is automatically re-registered at his or her new address.

- When a voter surrenders his or her Michigan Driver's license in a different state, the Michigan Department of State receives this information. The Bureau of Elections uses this as initial information that the voter may have moved. The Bureau sends a notice of cancellation to the voter's address in Michigan. If the voter does not respond and does have any voting activity by the second even-year November federal election following the notice, the voter's registration is cancelled. After the notice is sent, the voter is marked inactive and can still vote until the cancellation occurs.
- When election mail (such as a voter information card or absent voter ballot application) sent to a voter by a clerk is returned by the United States Postal Service as undeliverable, clerks use this as initial information that the voter may have moved. The clerk sends a notice of cancellation to the voter's address in Michigan. If the voter does not respond and does have any voting activity by the second even-year federal election following the notice, the voter's registration is cancelled. After the notice is sent, the voter is marked inactive and can still vote until the cancellation occurs.

State and local election officials were able to identity a significant number of registered voters who appeared to have changed address through the statewide mailing of absent voter ballot applications in 2020, the first statewide election mailing in at least a decade. State and local officials used applications that were returned as undeliverable to mark voters as inactive and send notices of cancellation in 2021 and without action by these voters the registrations will be cancelled after the two-federal-election waiting period expires in 2024. Because of this, many more voter registrations were identified and will be cancelled after 2024 than after 2022.

Another large-scale election mailing is ongoing prior to the 2022 election. Because of redistricting, most voters have either a new precinct or polling place, or at least one new election district. When this happens, the clerk sends the voter a new voter information card (also known as a voter id card) with the voter's new voting information. (See illustration above)

Under the Michigan Election Law these notices must be sent to all registered voters including inactive voters. When these voter information cards are returned undeliverable, clerks will inactivate the voters' registrations and send them notices of cancellation; these voters will also be scheduled for cancellation after 2024.

Michigan also receives information from the Electronic Registration Information Center (ERIC), a bipartisan group of 31 states and Washington, DC, who share voter registration data with each other for the purpose of keeping voter rolls complete, up to date, and accurate. When Michigan receives information through the ERIC program that a voter has registered in another state more recently than their activity in Michigan, the Bureau of Elections uses this as initial information that the voter may have moved. The Bureau sends a notice of cancellation to the voter's address in Michigan. If the voter does not respond and does have any voting activity by the second even-year federal election following the notice, the voter's registration is cancelled. After the notice is sent, the voter is marked inactive and can still vote until the cancellation occurs.

Election officials also have multiple ways of identifying voters who die.

- When someone dies and their death record is processed, this information is sent to the Social Security Administration and added to the Master Death Index. The Michigan Department of State receives this information from the Social Security Administration. On a weekly basis, the Bureau of Elections cancels the voter registrations of all registered voters who appear on the Master Death Index report.
- County clerks also inform a city or township clerks when they process death records for an individual registered to vote in that city or township. Although the vast majority of these deceased individuals are also identified through the Master Death Index, county clerks may be able to provide this information to municipal clerks most quickly. This is useful in the

AMERICAN OVERSIGHT

days leading up to elections, to allow the registrations of voters who become deceased to be cancelled more quickly.

- ✦ City or Township clerks can also cancel registrations when they have personal knowledge that a registered voter has become deceased. For example, the city or township clerk may have an obituary, local death notice, or a written notification from next of kin.
- ✦ Michigan also receives information from the ERIC program about Michigan voters who have died.
- ✦ There are additional inactive registrations in QVF for voters who may have died or moved, but for whom death or residency information was never received by election officials. If an election official receives returned undeliverable mail for these individuals, the registration will be cancelled two federal election cycles after the notification is sent unless the voter responds or has voting activity. Election officials have also requested legislative changes that would allow additional methods of identifying, notifying, and eventually cancelling these registrations.

Election officials also use multiple procedures to prevent duplicate registrations and merge registration records when the duplicate is identified.

- ✦ Whenever a new registration is processed in the Qualified Voter File, the file performs a match of the Voter File to determine if a registration already exists for that individual. If it does, the existing registration record is updated rather than a new registration record being created.
- ✦ If a clerk believes a duplicate registration exists, the clerk notifies the Bureau of Elections. The Bureau researches the record to determine if there are duplicate registrations for the same individual, or if they are actually two individuals with similar names.
- ✦ If the Bureau determines that an individual has duplicate registrations, the registration records are merged into one registration record.

Voters can also request that their registrations be cancelled.

- ✦ Voters who wish to cancel their registrations can make a written request to their city or township clerk that their registration record be cancelled.
- ✦ Voters who have received a notice of cancellation can respond to the notice confirming that their registration should be cancelled. This results in the registration being cancelled immediately, rather than at the end of the two-election waiting period.

Voter registration Statistics The total number of registered voters in Michigan is over 8 million. Go to Voter registration statistics to see the current number and for a list of registered voters by county and for the total number of inactive voter registrations to be cancelled in 2023 and 2025.

What to do if you receive election mail for someone who no longer lives there. If you receive election mail for someone who no longer lives at your address, you have the opportunity to assist the U.S. Postal Service and your local clerk in updating the voter rolls. You should write "no longer at this address" on the piece of mail and put it back in the mailbox. The U.S. Postal Service will then notify your local clerk that election mail for that registered voter has been returned as undeliverable. The clerk will then send a notice of cancellation which will result in that registration being cancelled after two federal elections have passed.

If someone at the residence is deceased, you can write "deceased" on the piece of mail and put it back in the mailbox. If a family member in your residence has died, you can also contact your clerk in writing and inform them that the family member is deceased. You can also send an obituary or death notice to the clerk, who can use this information to cancel the voter registration, so your household no longer receives election mail for the person who has passed away.

What to do if you receive a notice of cancellation. If you receive a notice of cancellation mailing for your own voter registration, you can respond to the notification by mail or online, and you have the following options as to what you respond:

AMERICAN OVERSIGHT

~ Copyright by Sharon Lawrence 110 ~

- ✦ Request your voter registration be cancelled. If you select this option, your voter registration will be cancelled immediately.
- ✦ Update your voter registration. If you have moved, you can update your voter registration to your new address.
- ✦ Vote or request an absent voter ballot in an upcoming election. This will keep your voter registration active and your registration will not be cancelled.
- ✦ Do nothing. If you don't respond and don't vote or request an absent voter ballot in an upcoming election, your registration will be cancelled after the second federal (even year November) election after you get the notice.

What to do if you haven't gotten a notice, but wish to cancel your registration. If you want to cancel your voter registration immediately but you haven't received a notice, you can contact your clerk in writing and request that your registration be cancelled.

What to do if your registration has been cancelled but you want to vote. If your registration has been cancelled but you still want to vote in Michigan, you will need to re-register. You can register to vote online or through any method of voter registration up to 15 days before an election. Within 14 days of an election, including on Election Day, you can register to vote at your city or township clerk's office with residency verification. For more information, go to registering to vote.

Why is there a two-election waiting period before cancelling registrations for voters who move? Both state and federal law require election officials to wait two federal elections before cancelling the registration of voters where the election official has received initial information that the person *may* have moved. The waiting period is required because sometimes the initial information suggesting that someone has moved does not mean they have actually changed their voting residency. For example, mail may be returned as undeliverable by mistake and the voter actually lives at the address. Or, someone may have changed their address for one purpose (such as a temporary work assignment, school, or military service) but they actually wish to continue voting in Michigan.

In addition, some voters who live in foreign countries may not have a U.S. address and they use their last U.S. address for voting residency purposes. Therefore, it is possible that someone who used to live at your residence is still legally using that address as their voting residence in Michigan, even though the person is currently living in a foreign country.

2021 Voter Cancellation. In March 2021, the Michigan Bureau of Elections canceled approximately 177,000 Michigan voter registrations as part of routine, post-election voter list maintenance. The registrations belong to people who appear to have moved, because before the November 2018 election they surrendered a Michigan driver's license in another state or had election mail sent to them and returned to an election official as undeliverable.

As required by federal law, these voters were sent a notice prior to the November 2018 election, did not respond to the notice, and have not voted or had other voting activity in at least the last two federal election cycles (2020 and 2018). Voters canceled by this list will need to contact their local clerk to re-register. Voters can find their local clerk by clicking on "Your Clerk" at Michigan.gov/Vote. Voters can also use that site to update their registration if they have moved to a different address in Michigan.

~ Copyright by Sharon Lawrence 111 ~

AMERICAN OVERSIGHT



In closing, a final word of appreciation to those who run for office and those who support them!

~ Copyright by Sharon Lawrence 112 ~

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
All States	Local Officials	https://www.usvotefoundation.org/vote/eoddomestic.htm
Alabama	Ballot Tracking	https://myinfo.alabamavotes.gov/voterview
Alabama	Elections Agency	Secretary of State
Alabama	Local Officials	https://www.sos.alabama.gov/city-county-lookup
Alabama	Main Website	https://www.sos.alabama.gov/alabama-votes
Alabama	Voter Guide	https://www.sos.alabama.gov/sites/default/files/election-2022/2022%20Voter%20Guide.pdf
Alabama	Voter Registration	https://www.sos.alabama.gov/alabama-votes/voter/register-to-vote
Alabama	Voter Registration	https://www.alabaMain Websiteteractive.org/sos/voter_registration/voterRegistrationWelcome.action
Alaska	Ballot Tracking	https://myvoterinformation.alaska.gov/
Alaska	Elections Agency	Lieutenant Governor
Alaska	Local Officials	
Alaska	Main Website	https://www.elections.alaska.gov/
Alaska	Voter Guide	https://www.elections.alaska.gov/Core/officialelectionpamphlets.php
Alaska	Voter Registration	https://voterregistration.alaska.gov/
Arizona	Ballot Tracking	https://my.arizona.vote/AbsenteeTracker.aspx
Arizona	Elections Agency	Secretary of State
Arizona	Local Officials	https://azsos.gov/county-election-info
Arizona	Main Website	https://azsos.gov/elections
Arizona	Main Website	https://www.azcleanelections.gov
Arizona	Voter Guide	
Arizona	Voter Registration	https://azsos.gov/elections/voting-election/register-vote-or-update-current-voter-information
Arkansas	Ballot Tracking	https://www.voterview.ar-nova.org/VoterView
Arkansas	Elections Agency	Secretary of State
Arkansas	Local Officials	https://www.sos.arkansas.gov/uploads/elections/County_Clerk_Contact_List_-_Rev._8-28-2020_.pdf
Arkansas	Main Website	https://www.sos.arkansas.gov/elections
Arkansas	Voter Guide	
Arkansas	Voter Registration	https://www.sos.arkansas.gov/elections/voter-information
California	Ballot Tracking	https://california.ballottrax.net/voter/
California	Elections Agency	Secretary of State
California	Local Officials	https://www.sos.ca.gov/elections/voting-resources/county-elections-offices
California	Main Website	https://www.sos.ca.gov/elections

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
California	Voter Guide	https://voterguide.sos.ca.gov/
California	Voter Registration	https://registertovote.ca.gov/
Colorado	Ballot Curing	https://www.coloradosos.gov/pubs/elections/FAQs/TXT2Cure.html (fix errors on mail & provisional ballots)
Colorado	Ballot Tracking	https://colorado.ballottrax.net/voter/
Colorado	Elections Agency	Secretary of State
Colorado	Local Officials	https://www.coloradosos.gov/pubs/elections/Resources/CountyElectionOffices.html
Colorado	Main Website	https://www.coloradosos.gov/pubs/elections/main.html
Colorado	Voter Guide	https://leg.colorado.gov/content/initiatives/initiatives-blue-book-overview/ballot-information-booklet-blue-book
Colorado	Voter Registration	https://www.coloradosos.gov/voter/pages/pub/home.xhtml
Connecticut	Ballot Tracking	https://portaldir.ct.gov/sots/LookUp.aspx
Connecticut	Elections Agency	Secretary of State
Connecticut	Local Officials	https://portal.ct.gov/SOTS/Election-Services/Find-Your-Town-Clerk-Registrar-and-Elected-Officials
Connecticut	Main Website	https://portal.ct.gov/SOTS/Common-Elements/V5-Template---Redesign/Elections--Voting--Home-Page
Connecticut	Main Website	https://portal.ct.gov/SOTS/Election-Services/Voter-Information/Voter-Fact-Sheet
Connecticut	Voter Guide	
Connecticut	Voter Registration	https://voterregistration.ct.gov/OLVR/
Delaware	Ballot Tracking	https://ivote.de.gov/VoterView
Delaware	Elections Agency	State Election Commissioner
Delaware	Local Officials	https://elections.delaware.gov/locations.shtml
Delaware	Main Website	https://elections.delaware.gov/
Delaware	Voter Guide	
Delaware	Voter Registration	https://ivote.de.gov/VoterView
Florida	Ballot Tracking	https://dos.myflorida.com/elections/for-voters/check-your-voter-status-and-polling-place/vote-by-mail-ballot-information-and-status-lookup/
Florida	Elections Agency	Secretary of State
Florida	Local Officials	https://dos.myflorida.com/elections/for-voters/check-your-voter-status-and-polling-place/vote-by-mail-ballot-information-and-status-lookup/
Florida	Main Website	https://dos.myflorida.com/elections/
Florida	Main Website	https://registration.elections.myflorida.com/CheckVoterStatus
Florida	Voter Guide	https://dos.myflorida.com/elections/forms-pub (Constitutional amendments booklet)
Florida	Voter Registration	https://dos.myflorida.com/elections/for-voters/voter-registration/
Georgia	Ballot Tracking	https://mvp.sos.ga.gov/s/
Georgia	Elections Agency	Secretary of State

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Georgia	Local Officials	https://sos.ga.gov/county-elections-offices
Georgia	Main Website	https://sos.ga.gov/elections-division-georgia-secretary-states-office
Georgia	Voter Guide	
Georgia	Voter Registration	https://sos.ga.gov/how-to-guide/how-guide-registering-vote
Hawaii	Ballot Tracking	https://ballotstatus.hawaii.gov/ballotreceipt
Hawaii	Elections Agency	Chief Election Officer
Hawaii	Local Officials	https://elections.hawaii.gov/voter-service-centers-and-places-of-deposit/
Hawaii	Main Website	https://elections.hawaii.gov/
Hawaii	Voter Guide	
Hawaii	Voter Registration	https://elections.hawaii.gov/register-to-vote/registration/
Hawaii	Voter Registration	https://olvr.hawaii.gov/Default.aspx?redir=1
Idaho	Ballot Tracking	https://voteidaho.gov/online-voter-tools/ (click on "check voter record")
Idaho	Elections Agency	Secretary of State
Idaho	Local Officials	https://voteidaho.gov/county-clerks/
Idaho	Main Website	https://sos.idaho.gov/elections-division/
Idaho	Main Website	https://elections.sos.idaho.gov/ElectionLink/ElectionLink/VoterSearch.aspx
Idaho	Main Website	https://voteidaho.gov/
Idaho	Voter Guide	https://voteidaho.gov/citizens-guide/
Idaho	Voter Registration	https://voteidaho.gov/
Illinois	Ballot Tracking	https://www.elections.il.gov/VotingAndRegistrationSystems/ProvisionalBallotSearch.aspx?MID=msI25d5%2fk1Q%3d&T=638018717888089060
Illinois	Elections Agency	Executive Director
Illinois	Local Officials	https://www.elections.il.gov/ElectionOperations/ElectionAuthorities.aspx?MID=snNj91xkBrk%3d&T=638018717360648305
Illinois	Main Website	https://www.elections.il.gov/
Illinois	Voter Guide	https://votersguide.elections.il.gov/?T=638018716455542537
Illinois	Voter Registration	https://ova.elections.il.gov
Indiana	Ballot Tracking	https://indianavoters.in.gov/
Indiana	Elections Agency	Secretary of State
Indiana	Local Officials	https://indianavoters.in.gov/CountyContact/Index
Indiana	Main Website	https://www.in.gov/sos/elections/
Indiana	Main Website	https://indianavoters.in.gov/
Indiana	Voter Guide	
Indiana	Voter Registration	https://indianavoters.in.gov/

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Iowa	Ballot Tracking	https://sos.iowa.gov/elections/absenteeballotstatus/absentee/
Iowa	Elections Agency	Secretary of State
Iowa	Local Officials	https://sos.iowa.gov/elections/auditors/auditorslist.html
Iowa	Main Website	https://sos.iowa.gov/#
Iowa	Main Website	https://voterready.iowa.gov/
Iowa	Voter Guide	
Iowa	Voter Registration	https://sos.iowa.gov/elections/voterinformation/voterregistration.html
Kansas	Ballot Tracking	https://myvoteinfo.voteks.org/voterview/
Kansas	Elections Agency	Secretary of State
Kansas	Local Officials	https://www.sos.ks.gov/elections/county_election_officers.aspx
Kansas	Main Website	https://www.sos.ks.gov/elections/elections.html
Kansas	Main Website	https://myvoteinfo.voteks.org/voterview
Kansas	Voter Guide	
Kansas	Voter Registration	https://www.kdor.ks.gov/Apps/VoterReg
Kentucky	Ballot Tracking	https://vrsws.sos.ky.gov/VIC/
Kentucky	Elections Agency	Secretary of State
Kentucky	Local Officials	https://elect.ky.gov/About-Us/Pages/County-Clerks.aspx
Kentucky	Main Website	https://elect.ky.gov/Pages/default.aspx
Kentucky	Main Website	https://vrsws.sos.ky.gov/ovrweb/govoteky
Kentucky	Voter Guide	
Kentucky	Voter Registration	https://vrsws.sos.ky.gov/ovrweb/
Louisiana	Ballot Tracking	https://voterportal.sos.la.gov/MobileLanding.aspx
Louisiana	Elections Agency	Secretary of State
Louisiana	Local Officials	https://voterportal.sos.la.gov/registrar
Louisiana	Main Website	https://www.sos.la.gov/ElectionsAndVoting/Pages/default.aspx
Louisiana	Main Website	https://voterportal.sos.la.gov/Home/VoterLogin
Louisiana	Voter Guide	https://www.sos.la.gov/ElectionsAndVoting/PublishedDocuments/VotingInLouisianaWeb.pdf
Louisiana	Voter Registration	https://www.sos.la.gov/ElectionsAndVoting/RegisterToVote/Pages/default.aspx
Maine	Ballot Tracking	https://apps.web.maine.gov/cgi-bin/online/AbsenteeBallot/ballot_status.pl
Maine	Elections Agency	Secretary of State
Maine	Local Officials	https://www.maine.gov/portal/government/edemocracy/voter_lookup.php

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Maine	Main Website	https://www.maine.gov/sos/cec/elec/index.html
Maine	Main Website	https://www.maine.gov/portal/government/edemocracy/voter_lookup.php
Maine	Voter Guide	
Maine	Voter Registration	https://www.Main Websitee.gov/sos/cec/elec/voter-info/voterguide.html
Maryland	Ballot Tracking	https://voterservices.elections.maryland.gov/VoterSearch
Maryland	Elections Agency	Board of Elections
Maryland	Local Officials	https://www.maine.gov/sos/cec/elec/munic.html
Maryland	Main Website	https://elections.maryland.gov/
Maryland	Voter Guide	
Maryland	Voter Registration	https://elections.maryland.gov/voter_registration/index.html
Massachusetts	Ballot Tracking	https://www.sec.state.ma.us/wheredoivotema/track/trackmyballot.aspx
Massachusetts	Elections Agency	Secretary of Commonwealth
Massachusetts	Local Officials	https://www.sec.state.ma.us/ele/eleev/ev-find-my-election-office.htm
Massachusetts	Main Website	https://www.sec.state.ma.us/ele/eleidx.htm
Massachusetts	Voter Guide	
Massachusetts	Voter Registration	https://www.sec.state.ma.us/OVR/
Michigan	Ballot Tracking	https://mvic.sos.state.mi.us/Voter/Index
Michigan	Elections Agency	Secretary of State
Michigan	Local Officials	https://mvic.sos.state.mi.us/Voter/Index/#yourclerk
Michigan	Main Website	https://www.michigan.gov/sos/elections
Michigan	Voter Guide	
Michigan	Voter Registration	https://mvic.sos.state.mi.us/RegisterVoter/Index
Michigan	Main Website	https://mvic.sos.state.mi.us/
Minnesota	Ballot Tracking	https://mnvotes.sos.state.mn.us/AbsenteeBallotStatus.aspx
Minnesota	Elections Agency	Secretary of State
Minnesota	Local Officials	https://www.sos.state.mn.us/elections-voting/find-county-election-office/
Minnesota	Main Website	https://sos.mn.gov/elections-voting/
Minnesota	Voter Guide	
Minnesota	Voter Registration	https://www.sos.state.mn.us/elections-voting/register-to-vote/
Mississippi	Ballot Tracking	
Mississippi	Elections Agency	Secretary of State

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Mississippi	Local Officials	https://www.sos.ms.gov/elections-voting/county-election-information
Mississippi	Main Website	https://www.sos.ms.gov/elections-voting
Mississippi	Main Website	https://www.sos.ms.gov/yall-vote
Mississippi	Voter Guide	https://www.sos.ms.gov/content/documents/Elections/VoterInformationGuide.pdf
Mississippi	Voter Registration	https://www.sos.ms.gov/index.php/elections-voting/voter-registration-information
Missouri	Ballot Tracking	
Missouri	Elections Agency	Secretary of State
Missouri	Local Officials	https://www.sos.mo.gov/elections/goVoteMissouri/localelectionauthority
Missouri	Main Website	https://www.sos.mo.gov/elections
Missouri	Voter Guide	
Missouri	Voter Registration	https://www.sos.mo.gov/elections/goVoteMissouri/register
Montana	Ballot Tracking	https://app.mt.gov/voterinfo/
Montana	Elections Agency	Secretary of State
Montana	Local Officials	https://app.mt.gov/voterinfo/
Montana	Main Website	https://sosmt.gov/elections/
Montana	Voter Guide	https://sosmt.gov/elections/vip/
Montana	Voter Registration	https://sosmt.gov/elections/vote/
Nebraska	Ballot Tracking	https://www.votercheck.necvr.ne.gov/voterview
Nebraska	Elections Agency	Secretary of State
Nebraska	Local Officials	https://sos.nebraska.gov/elections/election-officials-contact-information
Nebraska	Main Website	https://sos.nebraska.gov/
Nebraska	Voter Guide	
Nebraska	Voter Registration	https://www.nebraska.gov/apps-sos-voter-registration/
Nevada	Ballot Tracking	https://nevada.ballottrax.net/voter/
Nevada	Elections Agency	Secretary of State
Nevada	Local Officials	https://www.nvsos.gov/sos/elections/voters/county-clerk-contact-information
Nevada	Main Website	https://www.nvsos.gov/sos/elections
Nevada	Voter Guide	
Nevada	Voter Registration	https://www.nvsos.gov/sos/elections/voters/registering-to-vote
New Hampshire	Ballot Tracking	
New Hampshire	Elections Agency	Secretary of State

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
New Hampshire	Local Officials	https://app.sos.nh.gov/clerkinformation
New Hampshire	Main Website	https://www.sos.nh.gov/elections
New Hampshire	Voter Guide	
New Hampshire	Voter Registration	https://www.sos.nh.gov/elections/voters/register-vote
New Jersey	Ballot Tracking	https://www.nj.gov/state/elections/vote-track-my-ballot.shtml
New Jersey	Elections Agency	Secretary of State
New Jersey	Local Officials	https://nj.gov/state/elections/vote-county-election-officials.shtml
New Jersey	Main Website	https://nj.gov/state/elections/index.shtml
New Jersey	Main Website	https://nj.gov/state/elections/vote.shtml
New Jersey	Voter Guide	
New Jersey	Voter Registration	https://nj.gov/state/elections/voter-registration.shtml
New Mexico	Ballot Tracking	https://voterportal.servis.sos.state.nm.us
New Mexico	Elections Agency	Secretary of State
New Mexico	Local Officials	https://www.sos.state.nm.us/voting-and-elections/voter-information-portal/county-clerk-information/
New Mexico	Main Website	https://www.sos.state.nm.us/voting-and-elections/voter-information-portal/
New Mexico	Voter Guide	
New Mexico	Voter Registration	https://www.sos.state.nm.us/voting-and-elections/voter-information-portal/voter-registration-information/
New York	Ballot Tracking	https://nysballot.elections.ny.gov/TrackMyBallot/Search
New York	Elections Agency	Board of Elections
New York	Local Officials	
New York	Main Website	https://www.elections.ny.gov/
New York	Voter Guide	
New York	Voter Registration	https://www.elections.ny.gov/VotingRegister.html
North Carolina	Ballot Tracking	https://northcarolina.ballottrax.net/voter/
North Carolina	Elections Agency	Secretary of State
North Carolina	Local Officials	https://vt.ncsbe.gov/BOEInfo/
North Carolina	Main Website	https://www.ncsbe.gov/
North Carolina	Voter Guide	
North Carolina	Voter Registration	https://www.ncsbe.gov/registering/how-register
North Dakota	Ballot Tracking	https://vip.sos.nd.gov/AbsenteeTracker.aspx
North Dakota	Elections Agency	Secretary of State

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
North Dakota	Local Officials	https://vip.sos.nd.gov/CountyAuditors.aspx?ptlhPKID=34&ptlPKID=5
North Dakota	Main Website	https://sos.nd.gov/elections.html
North Dakota	Main Website	https://vip.sos.nd.gov/PortalList.aspx
North Dakota	Voter Guide	
North Dakota	Voter Registration	N/A
Ohio	Ballot Tracking	https://www.sos.state.oh.us/elections/voters/toolkit/ballot-tracking/
Ohio	Elections Agency	Secretary of State
Ohio	Local Officials	https://www.sos.state.oh.us/elections/elections-officials/county-boards-of-elections-directory/
Ohio	Main Website	https://www.sos.state.oh.us/elections/
Ohio	Voter Guide	
Ohio	Voter Registration	https://olvr.ohiosos.gov/
Oklahoma	Ballot Tracking	https://okvoterportal.okelections.us/
Oklahoma	Elections Agency	Secretary of State Senate
Oklahoma	Local Officials	
Oklahoma	Main Website	https://oklahoma.gov/elections.html
Oklahoma	Main Website	https://okvoterportal.okelections.us/
Oklahoma	Voter Guide	
Oklahoma	Voter Registration	https://oklahoma.gov/elections/voter-registration/register-to-vote.html
Oregon	Ballot Tracking	https://secure.sos.state.or.us/orestar/vr/showVoterSearch.do
Oregon	Elections Agency	Secretary of State
Oregon	Local Officials	https://sos.oregon.gov/elections/Pages/countyofficials.aspx
Oregon	Main Website	https://sos.oregon.gov/voting-elections/Pages/default.aspx
Oregon	Voter Guide	https://www.oregonvotes.gov/voters-guide/english/votersguide.html
Oregon	Voter Registration	https://secure.sos.state.or.us/orestar/vr/register.do?lang=eng&source=SOS
Pennsylvania	Ballot Tracking	https://www.pavoterservices.pa.gov/pages/ballottracking.aspx
Pennsylvania	Elections Agency	Secretary of State
Pennsylvania	Local Officials	https://www.vote.pa.gov/Resources/Pages/Contact-Your-Election-Officials.aspx
Pennsylvania	Main Website	https://www.dos.pa.gov/VotingElections/Pages/default.aspx
Pennsylvania	Main Website	https://www.vote.pa.gov
Pennsylvania	Voter Guide	
Pennsylvania	Voter Registration	https://www.pavoterservices.pa.gov/Pages/VoterRegistrationApplication.aspx

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Rhode Island	Ballot Tracking	https://vote.sos.ri.gov/Home/UpdateVoterRecord?ActiveFlag=3
Rhode Island	Elections Agency	Secretary of State & Board of Elections
Rhode Island	Local Officials	https://vote.sos.ri.gov/Elections/LocalBoards
Rhode Island	Main Website	https://vote.sos.ri.gov/
Rhode Island	Main Website	https://elections.ri.gov/
Rhode Island	Voter Registration	https://vote.sos.ri.gov/Home/RegistertoVote?ActiveFlag=1
South Carolina	Ballot Tracking	https://info.scvotes.sc.gov/eng/voterinquiry/VoterInformationRequest.aspx?
South Carolina	Elections Agency	Secretary of State & Elections Commission
South Carolina	Local Officials	https://scvotes.gov/contact/county-voter-registration-election-offices/
South Carolina	Main Website	https://scvotes.gov/
South Carolina	Voter Guide	
South Carolina	Voter Registration	https://scvotes.gov/voters/register-to-vote/
South Dakota	Ballot Tracking	https://vip.sdsos.gov/VIPLogin.aspx
South Dakota	Elections Agency	Secretary of State
South Dakota	Local Officials	https://vip.sdsos.gov/CountyAuditors.aspx
South Dakota	Main Website	https://sdsos.gov/elections-voting/default.aspx
South Dakota	Main Website	https://vip.sdsos.gov/VIPLogin.aspx
South Dakota	Voter Guide	https://sdsos.gov/elections-voting/assets/BallotQuestionPamphlet2022General.pdf (Ballot Questions Only)
South Dakota	Voter Registration	https://sdsos.gov/elections-voting/voting/register-to-vote/default.aspx
Tennessee	Ballot Tracking	https://tnmap.tn.gov/voterlookup/
Tennessee	Elections Agency	Secretary of State
Tennessee	Local Officials	https://tnsos.org/elections/election_commissions.php
Tennessee	Main Website	https://sos.tn.gov/elections
Tennessee	Main Website	https://sos.tn.gov/govotetn
Tennessee	Voter Guide	
Tennessee	Voter Registration	https://sos.tn.gov/elections/guides/how-to-register-to-vote
Texas	Ballot Tracking	https://teamrv-mvp.sos.texas.gov/BallotTrackerApp/#/login
Texas	Elections Agency	Secretary of State
Texas	Local Officials (Elections	https://www.sos.texas.gov/elections/voter/county.shtm
Texas	Local Officials (VR)	lhttps://www.sos.texas.gov/elections/voter/votregduties.shtml
Texas	Main Website	https://www.sos.state.tx.us/elections/index.shtml
Texas	Main Website	https://www.votetexas.gov/

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
Texas	Voter Guide	
Texas	Voter Registration	https://www.votetexas.gov/register-to-vote/index.html
Utah	Ballot Tracking	https://votesearch.utah.gov/voter-search/search/search-by-voter/track-mail-ballot
Utah	Elections Agency	Lieutenant Governor
Utah	Local Officials	https://voteinfo.utah.gov/county-clerk-contact-information/
Utah	Main Website	https://vote.utah.gov/
Utah	Voter Guide	https://voteinfo.utah.gov/wp-content/uploads/sites/42/2022/10/2022-VIP.pdf
Utah	Voter Registration	https://secure.utah.gov/voterreg/login.html?selection=REGISTER
Vermont	Ballot Tracking	https://mvp.vermont.gov/
Vermont	Elections Agency	Secretary of State
Vermont	Local Officials	https://sos.vermont.gov/elections/town-clerks/
Vermont	Main Website	https://sos.vermont.gov/elections/
Vermont	Voter Guide	
Vermont	Voter Registration	https://sos.vermont.gov/elections/voters/registration/
Virginia	Ballot Tracking	https://www.elections.virginia.gov/citizen-portal/
Virginia	Elections Agency	Board of Elections
Virginia	Local Officials	https://vote.elections.virginia.gov/VoterInformation/PublicContactLookup
Virginia	Main Website	https://www.elections.virginia.gov/
Virginia	Voter Guide	
Virginia	Voter Registration	https://www.elections.virginia.gov/registration/
Washington	Ballot Tracking	https://voter.votewa.gov/WhereToVote.aspx
Washington	Elections Agency	Secretary of State
Washington	Local Officials	https://www.sos.wa.gov/elections/auditors/
Washington	Main Website	https://www.sos.wa.gov/elections/
Washington	Voter Guide	https://www.sos.wa.gov/elections/voters-guide/2020/2020-general-election-voters-guide.aspx
Washington	Voter Registration	https://olvr.votewa.gov/
West Virginia	Ballot Tracking	https://apps.sos.wv.gov/Elections/Voter/AbsenteeBallotTracking (Absentee Ballot)
West Virginia	Ballot Tracking	https://apps.sos.wv.gov/Elections/Voter/ProvisionalBallotSearch (Provisional Ballot)
West Virginia	Elections Agency	Secretary of State
West Virginia	Local Officials	https://sos.wv.gov/elections/Pages/CountyClerkDirectory.aspx

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
West Virginia	Main Website	https://sos.wv.gov/elections/Pages/GoVoteWV.aspx
West Virginia	Voter Guide	
West Virginia	Voter Registration	https://ovr.sos.wv.gov/Register/Landing
Wisconsin	Ballot Tracking	https://myvote.wi.gov/en-us/Track-My-Ballot
Wisconsin	Elections Agency	Elections Commission
Wisconsin	Local Officials	https://myvote.wi.gov/en-us/My-Municipal-Clerk
Wisconsin	Main Website	https://elections.wi.gov/elections
Wisconsin	Main Website	https://myvote.wi.gov/en-us/
Wisconsin	Voter Guide	
Wisconsin	Voter Registration	https://myvote.wi.gov/en-us/Register-To-Vote
Wyoming	Ballot Tracking	
Wyoming	Elections Agency	Secretary of State
Wyoming	Local Officials	https://sos.wyo.gov/Elections/Docs/WYCountyClerks.pdf
Wyoming	Main Website	https://sos.wyo.gov/Elections/Default.aspx
Wyoming	Voter Guide	https://sos.wyo.gov/Elections/Docs/2022/2022_Voter_Guide.pdf
Wyoming	Voter Registration	https://sos.wyo.gov/Elections/State/RegisteringToVote.aspx
DC	Ballot Tracking	https://votedc.ballottrax.net/voter/
DC	Elections Agency	Board of Elections
DC	Main Website	https://www.dcboe.org/
DC	Voter Guide	https://www.dcboe.org/getattachment/GeneralElection2022/DCBOE-Voter-Guide-Fall-2022-9-5x11-WEB.pdf.aspx?lang=en-US
DC	Voter Registration	https://dcboe.org/Voters/Register-To-Vote/Register-to-Vote
American Samoa	Main Website	https://aselectionoffice.gov/
American Samoa	Voter Registration	https://aselectionoffice.gov/node/3
Guam	Main Website	http://gec.guam.gov/
Guam	Voter Registration	https://gec.guam.gov/index.php/uncategorized/where-to-register/
Northern Mariana Islands	Main Website	https://www.votecnmi.gov.mp/
Northern Mariana Islands	Voter Registration	https://www.votecnmi.gov.mp/
Puerto Rico	Main Website	http://www.ceepur.org
Puerto Rico	Voter Registration	
Virgin Islands	Main Website	https://www.vivote.gov/
Virgin Islands	Voter Registration	https://www.vivote.gov/voters/register-vote

AMERICAN OVERSIGHT

Elections Websites

ELECTION INFORMATION - STATES & TERRITORIES		
State/Territory		**Primary Election Website(s)**
		Copyright by Sharon Lawrence (October 27, 2022)

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
All States	
Alabama	
Alabama	
Alabama	
Alabama	
Alabama	
Alabama	
Alabama	
Alaska	
Alaska	
Alaska	
Alaska	
Alaska	Audio & bilingual versions
Alaska	
Arizona	
Arizona	
Arizona	
Arizona	
Arizona	
Arizona	
Arizona	
Arkansas	
Arkansas	
Arkansas	
Arkansas	
Arkansas	
Arkansas	
California	
California	
California	
California	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
California	American Sign Language & bilingual editions
California	
Colorado	
Colorado	
Colorado	
Colorado	
Colorado	
Colorado	Audio version
Colorado	
Connecticut	
Connecticut	
Connecticut	
Connecticut	
Connecticut	
Connecticut	
Connecticut	
Delaware	
Delaware	
Delaware	
Delaware	
Delaware	
Delaware	
Florida	
Florida	
Florida	
Florida	
Florida	
Florida	
Florida	
Georgia	
Georgia	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Georgia	
Georgia	
Georgia	
Georgia	
Hawaii	
Hawaii	
Hawaii	
Hawaii	
Hawaii	
Hawaii	
Hawaii	
Idaho	
Idaho	
Idaho	
Idaho	
Idaho	
Idaho	
Idaho	Bilingual version (Spanish only)
Idaho	
Illinois	Provisional only
Illinois	
Illinois	
Illinois	
Illinois	Bilingual version (Spanish only)
Illinois	
Indiana	
Indiana	
Indiana	
Indiana	
Indiana	
Indiana	
Indiana	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Iowa	
Iowa	
Iowa	
Iowa	
Iowa	
Iowa	
Iowa	
Kansas	
Kansas	
Kansas	
Kansas	
Kansas	
Kansas	
Kansas	
Kentucky	
Kentucky	
Kentucky	
Kentucky	
Kentucky	
Kentucky	
Kentucky	
Louisiana	
Louisiana	
Louisiana	
Louisiana	
Louisiana	
Louisiana	
Louisiana	
Maine	
Maine	
Maine	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Maine	
Maine	
Maine	
Maine	
Maryland	
Maryland	
Maryland	
Maryland	
Maryland	
Maryland	
Massachusetts	
Massachusetts	
Massachusetts	
Massachusetts	
Massachusetts	
Massachusetts	
Michigan	
Michigan	
Michigan	
Michigan	
Michigan	
Michigan	
Michigan	
Minnesota	
Minnesota	
Minnesota	
Minnesota	
Minnesota	
Minnesota	
Mississippi	
Mississippi	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Mississippi	
Mississippi	
Mississippi	
Mississippi	
Mississippi	
Missouri	
Missouri	
Missouri	
Missouri	
Missouri	
Missouri	
Montana	
Montana	
Montana	
Montana	
Montana	Large print version
Montana	
Nebraska	
Nebraska	
Nebraska	
Nebraska	
Nebraska	
Nebraska	
Nevada	
Nevada	
Nevada	
Nevada	
Nevada	
Nevada	
New Hampshire	
New Hampshire	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
New Hampshire	
New Hampshire	
New Hampshire	
New Hampshire	
New Jersey	
New Jersey	
New Jersey	
New Jersey	
New Jersey	
New Jersey	
New Jersey	
New Mexico	
New Mexico	
New Mexico	
New Mexico	
New Mexico	
New Mexico	
New York	
New York	
New York	
New York	
New York	
New York	
North Carolina	
North Carolina	
North Carolina	
North Carolina	
North Carolina	
North Carolina	
North Dakota	
North Dakota	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
North Dakota	
North Dakota	
North Dakota	
North Dakota	
North Dakota	
Ohio	
Ohio	
Ohio	
Ohio	
Ohio	
Ohio	
Oklahoma	
Oklahoma	
Oklahoma	
Oklahoma	
Oklahoma	
Oklahoma	
Oklahoma	
Oregon	
Oregon	
Oregon	
Oregon	
Oregon	
Oregon	
Pennsylvania	
Pennsylvania	
Pennsylvania	
Pennsylvania	
Pennsylvania	
Pennsylvania	
Pennsylvania	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Rhode Island	
Rhode Island	
Rhode Island	
Rhode Island	
Rhode Island	
Rhode Island	
South Carolina	
South Carolina	
South Carolina	
South Carolina	
South Carolina	
South Carolina	
South Dakota	
South Dakota	
South Dakota	
South Dakota	
South Dakota	
South Dakota	
South Dakota	
Tennessee	Voter Registration Lookup
Tennessee	
Tennessee	
Tennessee	
Tennessee	
Tennessee	
Tennessee	
Texas	
Texas	
Texas	
Texas	
Texas	
Texas	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes
Texas	
Texas	
Utah	
Utah	
Utah	
Utah	
Utah	
Utah	
Vermont	
Vermont	
Vermont	
Vermont	
Vermont	
Vermont	
Virginia	
Virginia	
Virginia	
Virginia	
Virginia	
Virginia	
Washington	
Washington	
Washington	
Washington	
Washington	Audio, bilingual, print (31) & video versions
Washington	
West Virginia	
West Virginia	
West Virginia	
West Virginia	

AMERICAN OVERSIGHT

Elections Websites

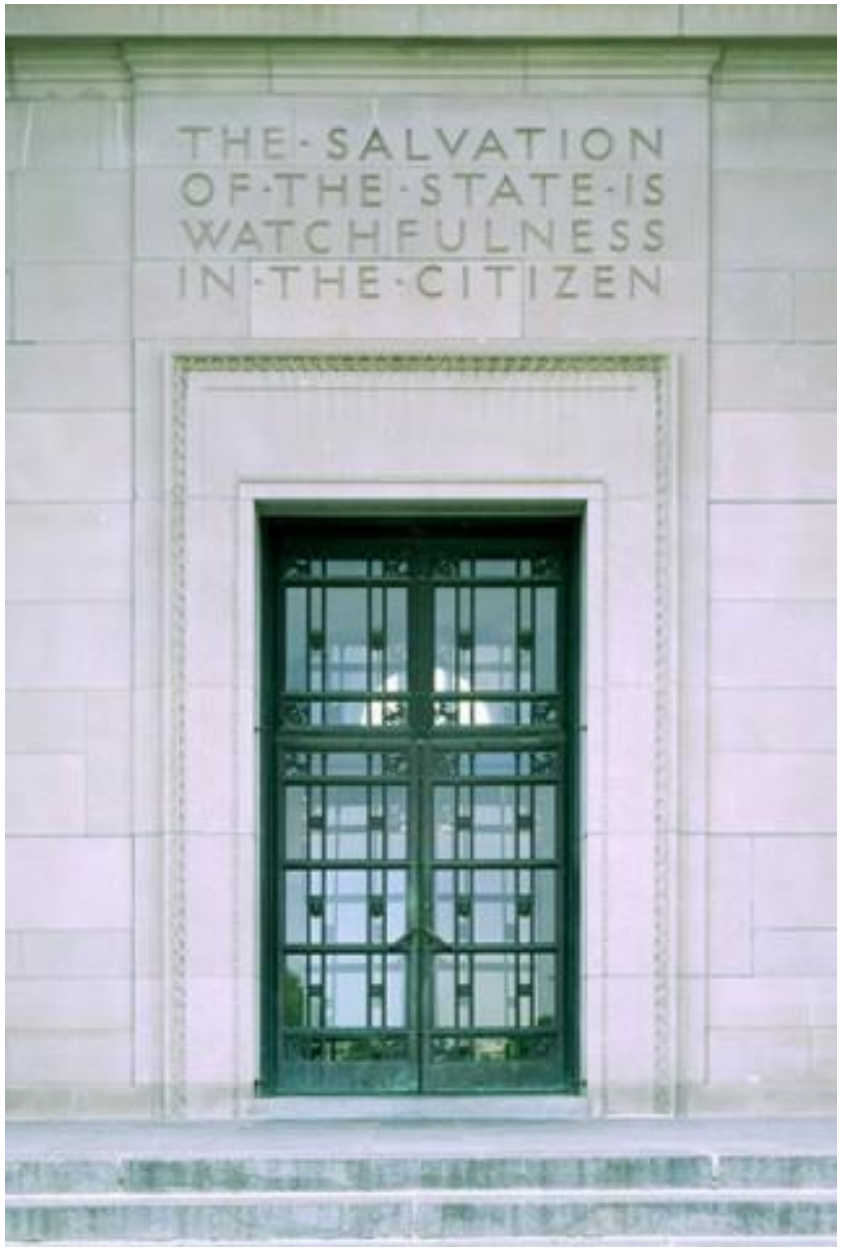
State/Territory	Notes
West Virginia	
West Virginia	
West Virginia	
Wisconsin	
Wisconsin	
Wisconsin	
Wisconsin	
Wisconsin	
Wisconsin	
Wisconsin	
Wyoming	
Wyoming	
Wyoming	
Wyoming	
Wyoming	
Wyoming	
DC	
DC	
DC	
DC	
DC	
American Samoa	
American Samoa	
Guam	
Guam	
Northern Mariana Islands	
Northern Mariana Islands	
Puerto Rico	
Puerto Rico	
Virgin Islands	
Virgin Islands	

AMERICAN OVERSIGHT

Elections Websites

State/Territory	Notes

AMERICAN OVERSIGHT



What's At Stake in the 2022 General Elections?

435 seats in the US House of Representatives
35 seats in the US Senate
36 Governors offices
30 Attorney General offices
27 Secretary of State positions
6,279 state legislative seats in 46 states
(not counting special elections)
72 State Supreme Court Judgeships

Sharon Lawrence
PO Box 387
San Marcos, TX 78667-0387
(512) 757-8669
https://www.linkedin.com/in/asksharonlawrence
(Last Updated: September 19, 2022)

AMERICAN OVERSIGHT

WHAT'S AT STAKE IN THE 2022 GENERAL ELECTION?[1]

State	US Senate	US House	Governor	Attorney General	Secretary of State	State Senate[2]	State Assembly/ House[3]	Supreme Court[4]
Alabama	Open	All	Incumbent	Incumbent	Open	All (35)	All (105)	2
Alaska	Incumbent	All	Incumbent			19 of 20	All (40)	1-R
Arizona	Incumbent	All	Open	Open	Open	All (30)	All (60)	
Arkansas	Incumbent	All	Open	Open	Incumbent	All (35)	All (100)	3
California	Incumbent	All	Incumbent	Incumbent	Incumbent	20 of 40	All (80)	4-R
Colorado	Incumbent	All	Incumbent	Incumbent	Incumbent	28 of 35	All (65)	
Connecticut	Incumbent	All	Incumbent	Incumbent	Open	All (36)	All (151)	
Delaware		All		Incumbent		All (21)	All (41)	
Florida	Incumbent	All	Incumbent	Incumbent		All (40)	All (120)	5 – R
Georgia	Incumbent	All	Incumbent	Incumbent	Incumbent	All (56)	All (180)	
Hawaii	Incumbent	All	Open			All (25)	All (51)	
Idaho	Incumbent	All	Incumbent	Incumbent	Open	All (35)	All (70)	
Illinois	Incumbent	All	Incumbent	Incumbent	Open	All (59)	All (118)	4 – R
Indiana	Incumbent	All		Incumbent	Incumbent	25 of 50	All (100)	
Iowa	Incumbent	All	Incumbent		Incumbent	34 of 50	All (100)	2 – R
Kansas	Incumbent	All	Incumbent	Open	Incumbent	None (40)	All (125)	6 – R
Kentucky	Incumbent	All				19 of 38	All (100)	4

[1] Totals do not include special elections for State Senate and House seats (9 Senate & 2 Assembly/House seats).

[2] Senators in Arizona, Connecticut, Georgia, Idaho, Maine, Massachusetts, New Hampshire, New York, North Carolina, Rhode Island, South Dakota and Vermont serve two-year terms. All other Senators serve four-year terms. 1,973 total Senate seats.

[3] House members in Alabama, Louisiana (105), Maryland, and North Dakota serve four-year terms. 5,412 total House seats.

[4] Arkansas (3 – Nonpartisan), Georgia (3 – Nonpartisan), and Idaho (2 – Nonpartisan) conducted elections for Supreme Court positions earlier this year. R indicates a retention vote.

Judicial elections are partisan in Alabama, Illinois, Louisiana, New Mexico, North Carolina, Ohio, and Texas.

AMERICAN OVERSIGHT

Louisiana[5]	Incumbent	All				-- (39)	---- (105)	1[6]
Maine		All	Incumbent			All (35)	All (151)	
Maryland	Incumbent	All	Open	Open		All (47)	All (141)	1 – R
Massachusetts		All	Open	Open	Incumbent	All (40)	All (160)	
Michigan		All	Incumbent	Incumbent	Incumbent	All (38)	All (110)	2
Minnesota		All	Incumbent	Incumbent	Incumbent	All (67)	All (134)	2
Mississippi[7]		All				-- (52)	-- (122)	
Missouri	Open	All				17 of 34	All (163)	2 – R
Montana		All				25 of 50	All (100)	2
Nebraska		All	Open	Open	Incumbent	24 of 49	N/A	4 – R
Nevada	Incumbent	All	Incumbent	Incumbent	Open	11 of 21	All (42)	2
New Hampshire	Incumbent	All	Incumbent			All (24)	All (400)	
New Jersey[8]		All				-- (40)	-- (80)	
New Mexico		All	Incumbent	Open	Incumbent	None (42)	All (70)	3 – R
New York	Incumbent	All	Incumbent	Incumbent		All (63)	All (150)	
North Carolina	Open	All				All (50)	All (120)	2
North Dakota	Incumbent	All		Incumbent	Open	32 of 47	66 of 94	1
Ohio	Open	All	Incumbent	Incumbent	Incumbent	17 of 33	All (99)	3
Oklahoma	Incumbent Open	All	Incumbent	Incumbent		24 of 48	All (101)	4 – R
Oregon	Incumbent	All	Open			16 of 30	All (60)	
Pennsylvania	Open	All	Open			25 of 50	All (203)	
Rhode Island		All	Incumbent	Incumbent	Open	All (38)	All (75)	
South Carolina	Incumbent	All	Incumbent	Incumbent	Incumbent	None (46)	All (124)	
South Dakota	Incumbent	All	Incumbent	Open	Open	All (35)	All (70)	2 – R
Tennessee		All	Incumbent			17 of 33	All (99)	
Texas		All	Incumbent	Incumbent		All (31)	All (150)	6

5 Statewide elections are held in odd years.
6 Election will be December 10, 2022.
7 Statewide elections are held in odd years.
8 Statewide elections are held in odd years.

AMERICAN OVERSIGHT

Utah	Incumbent	All				14 of 29	All (75)	1 – R
Vermont	Open	All	Incumbent	Open	Open	All (30)	All (150)	
Virginia[9]		All				-- (40)	-- (100)	
Washington	Incumbent	All			Incumbent	25 of 49	All (98)	3
West Virginia		All				17 of 34	All (100)	
Wisconsin	Incumbent	All	Incumbent	Incumbent	Incumbent	16 of 33	All (99)	
Wyoming		All	Incumbent		Open	16 of 31	All (62)	
Total	**35**	**435**	**36**	**30**	**27**	**1,301 of 1,973**	**4,978 of 5,413**	**72**

Copyright by
Sharon Lawrence
PO Box 387
San Marcos, TX 78667-0387
(512) 757-8669
https://www.linkedin.com/in/asksharonlawrence

[9] Statewide elections are held in off years.

AMERICAN OVERSIGHT

From: Tammy Brown <tbrown@jcebmo.org>
To: Peters, Chrissy <chrissy.peters@sos.mo.gov>
Vincent, Trish <Trish.Vincent@sos.mo.gov>
Date: 9/26/2022 12:22:19 PM
Subject: American Policy Center
Attachments: American Policy Center.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

Here is the latest effort.

Tammy L. Brown
Director
Jackson County Board of
Election Commissioners
tbrown@jcebmo.org
816-325-4600

Disclaimer

The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by Mimecast Ltd, an innovator in Software as a Service (SaaS) for business. Providing a safer and more useful place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

AMERICAN OVERSIGHT

URGENT ACTION EVERY AMERICAN MUST TAKE TO SECURE THE NOVEMBER ELECTION

Few Americans know about the Electronic Registration Information Center (ERIC) and how it is being used to steal our elections. Tell your neighbors:

- ERIC was created as something that was supposed to "help" your state keep its voter lists free from ineligible voters. It does NOT! ERIC is a left-wing voter registration drive!
- 33 states and the District of Columbia are using taxpayer money to artificially inflate their voter rolls. Their names are what the Mules are dropping in ballot boxes, and who are voting millions of fraudulent mail-in ballots.
- ERIC members are forbidden to require a mark of citizenship with a name.
- Many thousands of voters are registered in more than one state, yet stay on the rolls of both and are provided ballots in each.
- Every state in the nation reports bloated voter rolls, many of which list more voters than the actual residents of voting age.
- ERIC state officials ignore these facts and act hostile and/or dismissive when questioned about it. And voter fraud is growing.

ERIC MUST BE STOPPED – HERE IS WHAT WE MUST DO:

- **Every State must withdraw from ERIC. It CAN be done! Louisiana quit ERIC on July 17, 2022, thanks to actions of local citizens.**

These are the 33 states that are members of ERIC and are using your tax dollars to enhance voter fraud:

Alabama, Alaska, Arizona, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Illinois, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Missouri, Nevada, New Jersey,

New Mexico, Ohio, Oregon, Pennsylvania, Rhode Island, South Carolina, Texas, Utah, Vermont, Virginia, Washington, West Virginia, and Wisconsin.

- Every governor must mandate that election supervisors conduct a comprehensive voter registration audit to accurately assess the quality of voter rolls and CLEAN them properly, as required by law.
- Allow only in-person voter registration in each state. NO THIRD-PARTY registration allowed (as is currently allowed in Florida, for example)
- Mandate that poll workers represent each party evenly.
- Mandate that poll-watchers be present during any ballot adjudications.
- ELIMINATE VOTING MACHINGS AND RETURN TO PAPER BALLOTS ONLY.
- Voting must occur on ONE day only. No early voting or drop boxes should be allowed. Absentee ballots must be applied for ahead of election day, and verified for eligible voters only.

WE MUST RETURN TO ELECTION BASICS THAT HAVE GUIDED THIS NATION FOR OVER 200 YEARS! We must pressure local and state election officials to return to fair and honest elections. Call your local Board of Elections. Contact your state representative. Let them know you are watching their actions and demand the actions above. Demand that your state quit ERIC.

Local action is the only way to secure our ballot boxes. Please join this effort today by making copies of this flyer and sharing it with as many friends, neighbors, and family as possible.

Prepared by the
American Policy Center
53 Main Street Box 3640
Warrenton, VA 20188
www.americanpolicy.org

American Policy Center

AMERICAN OVERSIGHT

From: kmuthig@eac.gov
To: Vincent, Trish <Trish.Vincent@sos.mo.gov>
Date: 8/9/2023 12:00:57 PM
Subject: August Newsletter: EAC Updates & Events

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please use Phish Alert to report it.

UPDATES & EVENTS

AUGUST 2023 NEWSLETTER

Highlights from this month's newsletter include:

- **National Poll Worker Recruitment Day is August 23!**
- **New Election Cybersecurity Allocability Underfunding Decision Policy**
- **Latest EAC Resources**
- **Blogs and Videos from the EAC Commissioners on Elections in College Communities, Mental Health, and the Americans with Disabilities Act**
- **Recaps of the EAC Data Summit, LLC Annual Meeting, and EAC Public Meeting on Voter Outreach and Engagement**
- **Upcoming Event EAC Public Meeting on Voting Accessibility scheduled for September 6**

AMERICAN OVERSIGHT

National Poll Worker Recruitment Day is August 23!

The EAC's third annual National Poll Worker Recruitment Day will be held on Wednesday, August 23, 2023. State and local election officials, civic organizations and others can use this national awareness day to encourage Americans to sign up to become poll workers in their communities for upcoming elections.

To help participate in this day, the EAC has created a highly customizable social media toolkit at **HelpAmericaVote.gov**. The toolkit is easily editable to meet the needs of your jurisdiction or organization. The sample posts cater to both Twitter/X and Facebook.

The EAC also offers a **Poll Worker Recruitment Lookup Tool** to help people interested in signing up to be poll workers find information for their local election offices. If you are an election official, please make sure to review your election office's poll worker information in the tool. Please send any updates to **helpamericavote@eac.gov**.

The EAC's Local Leadership Council (LLC) Holds its First In-Person Annual Meeting

In late July, the EAC's Local Leadership Council (LLC) held its first in-person annual meeting since the board was established in June 2021. The 100-member board of election officials from across the country gathered for the two-day meeting in Washington, D.C.

AMERICAN OVERSIGHT

The meeting included moderated discussions on topics such as training and workforce development, looking ahead to 2024, and making the LLC an effective advisory board. Additionally, LLC members elected their first executive officers.

Learn more about the LLC.

New Election Cybersecurity Allocability Underfunding Decision Policy

In July 2023, the U.S. Election Assistance Commission (EAC) voted unanimously to consider allowable cybersecurity enhancements direct costs and allow full allocability under HAVA Section 101(b)(1)(F) of HAVA when the costs are reasonable and necessary and when the cost is incurred specifically for the purpose of benefitting election administration. The vote does not change the applicability of the Uniform Guidance (2 CFR Part 200) to EAC grant funding.

In accordance with the **Commissioners' decision**, the EA Office of Grants Management, in consultation with the Office of General Counsel, shall provide guidance on how states may attest and document that expenditures qualify as direct costs for the purpose of allocation. Written guidance is forthcoming and will be posted on the EAC Website at **www.eac.gov/grants/grants-guidance**. Questions on this decision must be directed to the Office of Grants Management at **grants@eac.gov**.

LATEST EAC RESOURCES

New Study on Accessibility of Elections for Americans with Disabilities

The EAC, in partnership with Rutgers University, released a pair of reports examining voting accessibility and disability turnout in the 2022 election. The agency worked with Professors Lisa Schur, Douglas Kruse, and Mason Ameri of the Program for Disability Research at Rutgers University to conduct the study.

The researchers focused on voter accessibility in the 2022 election, comparing the results to the same post-election surveys that were conducted in 2020 and 2012. The survey covered topics such as voter turnout, difficulties voting, the need for assistance in voting, voting methods, and treatment by election officials. The researchers also analyzed 2022 voter turnout using U.S. Census data. The findings are critical for election officials who continuously work to meet the needs of their jurisdictions and make voting accessible to all eligible voters.

The reports and other information for **Disability and Voting Accessibility in the 2022 Elections** can be found on the EAC's website. For a quick look at the study, you can also check out the EAC's new blog post on the study at **Understanding Voting Accessibility in the 2022 Elections**.

60 Second Security Series on Physical Security

The EAC created this 60 Second Security Series to help election officials quickly identify and address potential security issues. Each topic includes a brief description, a list of security measures, and potential funding sources for making these improvements. The following resources discuss physical security measures.

- **Personal Security**: Election officials can use the proactive steps in this resource to improve their personal security, such as documenting and reporting every threat and developing a working relationship with federal, state, and local law enforcement.

- **Building Access**: Building access refers to the process of allowing or denying individuals access to enter specific physical facilities. Election officials, who are often responsible for maintaining the security of multiple facilities, may use this checklist to help secure an elections office, secure storage areas, equipment warehouses, or rooms that contain sensitive election items.

- **Deploying Assets**: Election administration requires deploying critical systems within the elections office, as well as in the field at polling locations, satellite offices, or mobile voting units. Election officials can use this resource to address security concerns

AMERICAN OVERSIGHT

- related to deploying assets.

More information about these and other election security best practices can be found at eac.gov/election-officials.

State Elections Policies Data Map

Because election policies differ by state, the EAC created an interactive map to quickly show how state policies and procedures vary. These include policies regarding:

- State Election Officials
- Local Election Officials
- Voter Registration
- In-Person Voting
- Voting by Mail
- Post-Election Processes

The data included in this map was compiled by the National Conference of State Legislatures (NCSL), as of September 8, 2022.
Check out the interactive map and view the full dataset.

Electronic Poll Book Report

Electronic poll books (e-poll books) are central to the in-person voting experience in a growing number of jurisdictions. Election officials have leveraged e-poll books to streamline the check-in process, reduce errors, automate ballot issuing, and collect and display critical data. This report provides information on increasing e-poll book adoption, functions e-poll books fulfill, and applicable state laws and regulations. Understanding the current e-poll book environment enables further assessment of risks, mitigation measures, best practices, and information gaps that require further research.

Read and download the E-Poll Book Report and **view State Certification Requirements for Electronic Poll Books**

NEW VIDEOS AND BLOGS FROM THE EAC COMMISSIONERS

EAC Commissioner Ben Hovland Spotlights Election Administration in College Towns

Commissioner Hovland hosted a panel with eight election officials about administering elections in college towns or jurisdictions with significant student populations. The panel discussed issues and challenges faced by college-aged voters in those locations, voter education and participation efforts, registration for out-of-state students versus in-state students, navigating those different rules across states, and more.

Read the blog and watch the video.

EAC Commissioner Thomas Hicks Interviews Clearinghouse Award Winners for Voter Accessibility Programs

In recognition of the 33rd anniversary of the Americans with Disabilities Act, Commissioner Thomas Hicks held a discussion with election officials Kevin Dragotto from Dubuque County, Iowa; and Antone White and Matt Kelly from Franklin County, Ohio, about their offices' **2022 Clearinghouse Award-winning voter accessibility programs**.

Mr. Dragotto highlighted the Dubuque County Auditor's Office's strategic partnership with the Dubuque County Disabilities Council. After assessing polling locations on Election Day, the partnership was able to determine that small changes like better placement of curbside voting signs, larger laminated elevator signs, and word changes could help improve the voting experience for all.

Mr. White and Mr. Kelly spoke about the Franklin County Board of Elections Early Vote Center's ADA Station, which is located directly inside of the center's main entrance and is equipped with seating so that voters do not have to stand or walk far to use voting equipment. It initially consisted of two check-in stations and three ADA accessible voting kiosks. Due to its popularity, the station was expanded to 12 additional kiosks.

Watch the full discussion.

EAC Commissioner Ben Hovland had a Conversation with Jason Kander on Elections and Mental Health

Commissioner Hovland interviewed Jason Kander, a military veteran and former Missouri Secretary of State, about mental health and how it relates to elections.

Mr. Kander shared his story about his post-traumatic stress disorder, emphasized how everyone has their own struggles, and underlined the importance of sharing experiences with others.

Read the blog and watch the video.

EAC EVENTS RECAP

The EAC Hosts a Public Meeting on Voter Education and Engagement

On August 2, the EAC hosted an in-person public meeting on how election officials can improve education and outreach efforts ahead of the EAC's **Poll Worker Recruitment Day** on August 23.

During the meeting, EAC Commissioners moderated three panels on innovation in voter outreach and engagement, voter education strategies

AMERICAN OVERSIGHT

and ideas for 2024, and the EAC's resources on poll worker recruitment. Panelists included state and local election administrators from Delaware, Montgomery County, Maryland, and Paulding County, Georgia. They were joined by professors from Mississippi State University and Connecticut College, who are leading the EAC's Voter Education Project.

EAC staff also served as panelists to discuss the agency's poll worker resources as well as the agency's College Poll Worker Grant Program—funded for the first time since 2010.
Watch the full event.

The EAC Data Summit Highlights How the U.S. Voted in the 2022 Midterms

On July 19, the EAC held a Data Summit featuring a review of the **Election Administration and Voting Survey (EAVS)** report, the nation's most comprehensive source of election administration data. During the Data Summit, election administrators, EAC staff, and election subject matter experts discussed how voting and election administration have changed since the last midterm election in 2018, the last presidential election in 2020, and how this information can be used to prepare for the 2024 presidential election.

Watch the full event.

SAVE THE DATE

AMERICAN OVERSIGHT

The EAC to Hold a Public Meeting on Voting Accessibility on September 6

On September 6, the EAC will hold a public meeting on breaking down accessibility and language barriers to voting. The meeting, which will be held at the agency's DC office, will include election officials, subject matter experts, and other stakeholders. It will also highlight the EAC's accessibility and language resources for voters and election officials, such as best practices guides, new research, and a first-of-its-kind video training series. This meeting will be live streamed on the **EAC's YouTube channel**.

Please register on the event page if you plan to attend in person.

U.S. Election Assistance Commission

633 3rd Street NW, Suite 200 • Washington, DC 20001

www.eac.gov

Were you forwarded this newsletter? Sign up here.

© 2023

This email was sent to trish.vincent@sos.mo.gov
U.S. Election Assistance Commission, 633 3rd Street NW, Suite 200, Washington, D.C. 20001, United States
Unsubscribe

AMERICAN OVERSIGHT