Subject: RE: Public Information Request (TX-SOS-24-0284) - SOS PIR 24-0343
Date: Thursday, April 11, 2024 at 1:54:55 PM Eastern Daylight Time
From: GeneralCounsel
To: AO Records
CC: GeneralCounsel
Attachments: 4-11-24 15 Day Letter to Requestor - American Oversight PIR 24-0343.pdf, 4-11-24 15 Day Letter to OAG - American Oversight PIR 24-0343.pdf, 4.11.24 Documents.zip

EXTERNAL SENDER

Good afternoon,

Please see the attached letters, and zipped folder containing documents, in response to your request for information under Chapter 552 of the Texas Government Code.

The responsive documents contain email addresses of the general public. An email address of a member of the public is confidential under section 552.137 of the Texas Government Code. The attorney general authorized all governmental bodies to withhold an email address of a member of the public without first requesting an attorney general opinion in Open Records Decision No. 684 (2009). Thus, this information has been redacted.

As stated in the attached letter, we require more time to continue reviewing our records and produce additional responsive information. We will provide you additional responsive documents on a rolling basis—to the extent such information is not excepted from disclosure under state or federal law—with our next production by 5:00 p.m. on May 2, 2024. *See* Tex. Gov't Code § 552.221(d).

Kind regards,

Jennifer Williams
Legal Assistant to the General Counsel
Office of the Texas Secretary of State

From: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Sent: Thursday, April 4, 2024 9:47 AM
To: 'AO Records' <records@americanoversight.org>
Cc: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Subject: RE: Public Information Request (TX-SOS-24-0284) - SOS PIR 24-0343

Good morning,

Please see the attached letter, with enclosure, in response to your request for information under Chapter 552 of the Texas Government Code. We will also provide you with a copy of our brief to the OAG on or before April 11, 2024.

As stated in the attached letter, we are processing the Request in accordance with the terms of the PIA. To that end, we require more time to review our records and produce responsive information. We will provide you responsive documents on a rolling basis—to the extent such information is not excepted from disclosure under state or federal law—with the first production by 5:00 p.m. on April 11, 2024. *See* Tex. Gov't Code § 552.221(d).

Kind regards,

Jennifer Williams
Legal Assistant to the General Counsel
Office of the Texas Secretary of State

From: GeneralCounsel
Sent: Tuesday, March 26, 2024 3:10 PM
To: 'AO Records' <records@americanoversight.org>
Subject: RE: Public Information Request (TX-SOS-24-0284)

Good afternoon,

This email acknowledges receipt of your request for information under the Public Information Act, Chapter 552 of the Texas Government Code (the "PIA"), which was received by the Office via email on March 20, 2024 (the "Request").

We will process your Request in accordance with the PIA and will let you know if we have any questions or need clarification. Our Office will be closed on Friday, March 29th in observance of Good Friday. You will receive a response from our Office on or before the 10th business day, April 4, 2024.

Kind regards,

Jennifer Williams
Legal Assistant to the General Counsel
Office of the Texas Secretary of State

From: AO Records <records@americanoversight.org>
Sent: Wednesday, March 20, 2024 3:02 PM
To: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Subject: Public Information Request (TX-SOS-24-0284)

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Public Information Officer,

Please find attached a request for records under Texas public records laws.

Sincerely,

Mariuxi Pintado I (she/hers)
Senior Paralegal I American Oversight
records@americanoversight.org
www.americanoversight.org I @weareoversight

Public Information Request: TX-SOS-24-0284

From: Kristi Hart
To: Julia Montes; Lillian Eder
Subject: FW: MASS EMAIL (CEO/CSO/PARTY CHAIRS): Advisory No. 2023-26: Voter Registration List Maintenance Under the National Voter Registration Act of 1993 (NVRA)
Date: Thursday, December 21, 2023 4:01:00 PM

We need to be sure all of our ladies read this and KNOW this information.

From: Texas Secretary of State Elections Division <TXSoSAgency@public.govdelivery.com>
Sent: Thursday, December 21, 2023 2:48 PM
To: Kristi Hart <KHart@sos.texas.gov>
Subject: MASS EMAIL (CEO/CSO/PARTY CHAIRS): Advisory No. 2023-26: Voter Registration List Maintenance Under the National Voter Registration Act of 1993 (NVRA)

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Having trouble viewing this email? View it as a Web page.

SoS Header - General

ELECTIONS DIVISION

TO: Texas Election Officials

FROM: Elections Division, Texas Secretary of State

SUBJECT: Advisory No. 2023-26: Voter Registration List Maintenance Under the National Voter Registration Act of 1993 (NVRA) and the Texas Election Code as it Pertains to the Primary Election and Primary Runoff Election

DATE: December 21, 2023

Dear Election Officials and Party Chairs,

Our office has released **Advisory No. 2023-26: Voter Registration List Maintenance Under the**

National Voter Registration Act of 1993 (NVRA) and the Texas Election Code as it Pertains to the Primary Election and Primary Runoff Election

When posted this advisory will be located on your Conducting Elections pages.

Please let us know if you have any questions or concerns.

Thank you,

Heidi Martinez

Managing Attorney – Elections Division

Office of the Texas Secretary of State

1019 Brazos Street | Rudder Building, 2nd Floor | Austin, Texas 78701 1.800.252.VOTE (8683)

elections@sos.texas.gov | www.sos.state.tx.us/elections

The information contained in this email is intended to provide advice and assistance in election matters per §31.004 of the Texas Election Code. It is not intended to serve as a legal opinion for any matter. Please review the law yourself, and consult with an attorney when your legal rights are involved.

If you have any questions regarding this e-mail, please e-mail elections@sos.texas.gov

Stay Connected with Texas Secretary of State:

SUBSCRIBER SERVICES:
Manage Subscriptions | Unsubscribe All | Help

From: Christina Adkins
To: ELEC Management
Cc: Adam Bitter; Alicia Pierce
Subject: FW: Update, 7/6: NASED Call Notes, Cait Conley to Join Next NASED Call 7/14 @ Noon ET, EAVS Survey Report Published, EAC Local Leadership Council Meeting 7/20-21, Meta Announces New Threads App, ACE Act Text, and More!
Date: Friday, July 7, 2023 3:47:07 PM
Attachments: ACE Act Bill Text.pdf
ACE Act Bill Summary.pdf
Importance: High

Hey folks – I get emails from NASED on a weekly basis. This one has some things that may be of interest to some of you all.

Thanks,

Christina

From: [redacted]
Sent: Thursday, July 6, 2023 6:01 PM
To: [redacted]
Subject: Update, 7/6: NASED Call Notes, Cait Conley to Join Next NASED Call 7/14 @ Noon ET, EAVS Survey Report Published, EAC Local Leadership Council Meeting 7/20-21, Meta Announces New Threads App, ACE Act Text, and More!
Importance: High

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Good afternoon, all!

I hope everyone had a safe July 4th.

- NASED Call:
  - Attached please find the notes from Friday's conversation. Our next call will be **Friday, July 14 at noon ET** and we will be joined by Cait Conley, Senior Advisor to CISA Director Jen Easterly, who is taking on an expanded role on election security as Kim Wyman departs for the private sector. Cait will join us for the first ~30 minutes to introduce herself to you and take questions. I believe she is also planning to attend the conference in Charleston later this month.
- EAC:
  - The EAC released the 2022 Election Administration and Voting Survey (EAVS) on

    Thursday.
  - The EAC will hold a Local Leadership Council meeting in DC on Thursday July 20- 21. The meeting will not be livestreamed but it is open to the public. The agenda is available here.
    - As a reminder, the Local Leadership Council was established in June 2021 and is comprised of 100 local election officials who are appointed by each state's association of local election officials. The current list of membership designees is available here.
- Meta:
  - Meta (Facebook's parent company) announced their new Twitter competitor app, Threads, yesterday. Threads is currently only available if you have an Instagram account. If your Instagram account is verified, your Threads account will also be verified. If your office needs to get its Instagram account verified, and by extension a Threads account, please contact Eva Guidarini (eguidarini@meta.com) and she can get that take care of for you.
    - If any of your offices are using Threads, I'd be interested in hearing about your experiences.
- Congress:
  - House Admin Majority staff shared the attached text of the American Confidence in Elections (ACE) Act and bill summary. I believe this will drop next week. If you have questions or feedback on the bill, please share them with Caleb Hayes (Caleb.Hays@mail.house.gov).
  - On July 10 at 2:30pm ET, House Admin will hold a field hearing in Atlanta, GA, The Path to Election Integrity Across America. The current witness list (subject to additions) is:
    - Hans von Spakovsky, Manager, The Heritage Foundation Election Law Reform Initiative and Senior Legal Fellow, Edwin Meese III Center for Legal and Judicial Studies
    - Dr. Kathleen Ruth, Vice Chair, Fulton County Elections Board
- Misc:
  - One of the US Supreme Court decisions that came down last week was Counterman v. Colorado, a case I flagged for you a few months ago because, while it's not directly elections-related, many of you have run into the issue of whether threats you/your office report meet the definition of a "true threat." Counterman repeatedly contacted a musician via Facebook, and the musician reported him to law enforcement; Counterman was convicted of stalking. He appealed on the grounds that the threats were not "true threats." I won't pretend to be a lawyer, but the Supreme Court found that Counterman's First Amendment rights had been violated and said that a person sending threats must intend to do harm.
  - Reminder that now is a good time to look at your state statutes around the Electoral Count Act and make sure that they comply with the Electoral Count Reform Act in advance of the presidential election next year. Kansas and Indiana both made modifications, North Carolina has some in progress.

Tomorrow (July 7) is the last day to register for the NASED conference at the early bird rate!

That’s all 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 [redacted]

[DISCUSSION DRAFT]

MAY 31, 2023

118TH CONGRESS
1ST SESSION

H. R. ____

To promote election integrity, voter confidence, and faith in elections by removing Federal impediments to, providing State tools for, and establishing voluntary considerations to support effective State administration of Federal elections, improving election administration in the District of Columbia, improving the effectiveness of military voting programs, and protecting political speech, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. STEIL introduced the following bill; which was referred to the Committee on ______________________________

A BILL

To promote election integrity, voter confidence, and faith in elections by removing Federal impediments to, providing State tools for, and establishing voluntary considerations to support effective State administration of Federal elections, improving election administration in the District of Columbia, improving the effectiveness of military voting programs, and protecting political speech, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''American Confidence in Elections Act'' or the ''ACE Act''.

SEC. 2. TABLE OF CONTENTS.

The table of contents of this Act is as follows:

Subtitle D—District of Columbia Election Integrity and Voter Confidence

"Subtitle C—Requirements for Elections in District of Columbia

Subtitle E—Administration of the Election Assistance Commission

"Part 7—General Requirements for Payments

Subtitle F—Prohibition on Involvement in Elections by Foreign Nationals

Subtitle G—Constitutional Experts Panel With Respect to Presidential Elections

TITLE II—MILITARY VOTING ADMINISTRATION

Subtitle A—Findings Relating to Military Voting

Subtitle B—GAO Analysis on Military Voting Access

TITLE III—PROTECTION OF POLITICAL SPEECH AND CAMPAIGN FINANCE REFORM

Subtitle A—Protecting Political Speech

Subtitle B—Prohibition on Use of Federal Funds for Congressional Campaigns

Subtitle C—Registration and Reporting Requirements

Subtitle D—Exclusion of Certain Amounts From Treatment as Contributions or Expenditures

Subtitle E—Prohibition on Issuance of Regulations on Political Contributions

Subtitle F—Miscellaneous Provisions

TITLE IV—ELECTION SECURITY

Subtitle A—Promoting Election Security

Subtitle B—Cybersecurity for Election Systems

TITLE V—SENSE OF CONGRESS WITH RESPECT TO ROLE OF STATES IN CONGRESSIONAL REDISTRICTING

SEC. 3. GENERAL FINDINGS.

Congress finds the following:

(1) According to Article 1, Section 4 of the Constitution of the United States, the States have the primary role in establishing ‘‘(t)he Times, Places and Manners of holding Elections for Senators and Representatives’’, while Congress has a purely secondary role in this space and must restrain itself from acting improperly and unconstitutionally.

(2) Federal election legislation should never be the first step and must never impose burdensome, unfunded Federal mandates on State and local elections officials. When Congress does speak, it must devote its efforts only to resolving highly significant and substantial deficiencies to ensure the integrity of our elections. State legislatures are the primary venues to establish rules for governing elections and correct most issues.

(3) All eligible voters who wish to participate must have the opportunity to vote, and all lawful votes must be counted.

(4) States must balance appropriate election administration structures and systems with accessible access to the ballot box.

(5) Political speech is protected speech.

(6) The First Amendment protects the right of all Americans to state their political views and donate money to the candidates, causes, and organizations of their choice without fear of retribution.

(7) Redistricting decisions are best made at the State level.

(8) States must maintain the flexibility to determine the best redistricting processes for the particular needs of their citizens.

(9) Congress has independent authority under the Fourteenth, Fifteenth, Nineteenth, Twenty-Fourth, and Twenty-Sixth Amendments to ensure elections are conducted without unlawful discrimination.

(10) The Voting Rights Act, which is not anchored in Article 1, Section 4 of the Constitution, has seen much success since its first passage in

1965, and Congress should continue to exercise its constitutional authority in this space as appropriate.

TITLE I—ELECTION ADMINISTRATION INTEGRITY

Subtitle A—Findings Relating to Election Administration

SEC. 101. FINDINGS RELATING TO ELECTION ADMINISTRATION.

(a) SENSE OF CONGRESS.—It is the sense of Congress that constitutional scholar Robert Natelson has done invaluable work with respect to the history and understanding of the Elections Clause.

(b) FINDINGS.—Congress finds the following:

(1) The Constitution reserves to the States the primary authority to set election legislation and administer elections—the ‘‘times, places, and manner of holding of elections’’—and Congress' power in this space is purely secondary to the States' power and is to be employed only in the direst of circumstances. History, precedent, the Framers' words, debates concerning ratification, the Supreme Court, and the Constitution itself make it exceedingly clear that Congress' power over elections is not unfettered.

(2) The Framing Generation grappled with the failure of the Articles of Confederation, which provided for only a weak national government incapable of preserving the Union. Under the Articles, the States had exclusive authority over Federal elections held within their territory; but, given the difficulties the national government had experienced with State cooperation (e.g., the failure of Rhode Island to send delegates to the Confederation Congress), the Federalists, including Alexander Hamilton, were concerned with the possibility that the States, in an effort to destroy the Federal government, simply might not hold elections or that an emergency, such as an invasion or insurrection, might prevent the operation of a State's government, leaving the Congress without Members and the Federal government unable to respond.

(3) Quite plainly, Alexander Hamilton, a leading Federalist and proponent of our Constitution, understood the Elections Clause as serving only as a sort of emergency fail-safe, not as a cudgel used to nationalize our elections process. Writing as Publius to the people of New York, Hamilton further expounds on the correct understanding of the Elections Clause: "T[he] natural order of the subject

leads us to consider, in this place, that provision of the Constitution which authorizes the national legislature to regulate, in the last resort, the election of its own members.''. Alexander Hamilton (writing as Publius), *Federalist* no. 59, *Concerning the Power of Congress to Regulate the Election of Members*, N.Y. PACKET (Fri., Feb. 22, 1788).

(4) When questioned at the States' constitutional ratifying conventions with respect to this provision, the Federalists confirmed this understanding of a constitutionally limited, secondary congressional power under Article 1, Section 4. (``[C]onvention delegate James McHenry added that the risk to the federal government [without a fail-safe provision] might not arise from state malice: An insurrection or rebellion might prevent a state legislature from administering an election.''); (``An occasion may arise when the exercise of this ultimate power of Congress may be necessary . . . if a state should be involved in war, and its legislature could not assemble, (as was the case of South Carolina and occasionally of some other states, during the [Revolutionary] war).''); (``Sir, let it be remembered that this power can only operate in a case of necessity, after the factious or listless disposition of a par-

ticular state has rendered an interference essential to the salvation of the general government.''). *See* Robert G. Natelson, *The Original Scope of the Congressional Power to Regulate Elections*, 13 U. PA. J. CONST. L. 1, 12–13 (Nov. 2010).

(5) John Jay made similar claims in New York. And, as constitutional scholar Robert Natelson notes in his invaluable article, *The Original Scope of the Congressional Power to Regulate Elections*, ''Alexander Contee Hanson, a member of Congress whose pamphlet supporting the Constitution proved popular, stated flatly that Congress would exercise its times, places, and manner authority only in cases of invasion, legislative neglect or obstinate refusal to pass election laws [providing for the election of Members of Congress], or if a state crafted its election laws with a 'sinister purpose' or to injure the general government.'' Cementing his point, Hanson goes further to decree, ''The exercise of this power must at all times be so very invidious, that congress will not venture upon it without some very cogent and substantial reason.''. Alexander Contee Hanson (writing as Astrides), *Remarks on the Proposed Plan: 31 January*, reprinted in John P. Kaminski, Gaspare J. Saladino, and Richard Leffler (eds.), *3*

Commentaries on the Constitution, public and private 18 December 1787 to 31 January 1788 522–26 (1984).

(6) In fact, had the alternate view of the Elections Clause been accepted at the time of the Constitution's drafting—that is, that it offers Congress unfettered power over Federal elections— it is likely that the Constitution would not have been ratified or that an amendment to this language would have been required.

(7) Indeed, at least seven of the original 13 States—over half and enough to prevent the Constitution from being ratified—expressed specific concerns with the language of the Elections Clause. *See* 1 Annals of Cong. 799 (1789), Joseph Gales (ed.) (1834). However, ''[l]eading Federalists...'' assured them ''...that, even without amendment, the [Elections] Clause should be construed as limited to emergencies''. Three States, New York, North Carolina, and Rhode Island, specifically made their ratification contingent on this understanding being made express. *Ratification of the Constitution by the State of New York* (July 26, 1788) (''Under these impressions and declaring that the rights aforesaid cannot be abridged or violated, and the Explanations afore-

said are consistent with the said Constitution, And in confidence that the Amendments which have been proposed to the said Constitution will receive early and mature Consideration: We the said Delegates, in the Name and in [sic] the behalf of the People of the State of New York Do by these presents Assent to and Ratify the said Constitution. In full Confidence . . . that the Congress will not make or alter any Regulation in this State respecting the times places and manner of holding Elections for Senators or Representatives unless the Legislature of this State shall neglect or refuse to make laws or regulations for the purpose, or from any circumstance be incapable of making the same, and that in those cases such power will only be exercised until the Legislature of this State shall make provision in the Premises''); *Ratification of the Constitution by the State of North Carolina* (Nov. 21, 1789) (''That Congress shall not alter, modify, or interfere in the times, places, or manner of holding elections for senators and representatives, or either of them, except when the legislature of any state shall neglect, refuse or be disabled by invasion or rebellion, to prescribe the same.''); *Ratification of the Constitution by the State of Rhode Island* (May 29, 1790) (''Under these impressions, and declaring, that the rights aforesaid cannot be abridged or violated, and that the explanations aforesaid, are consistent with the said constitution, and in confidence that the amendments hereafter mentioned, will receive an early and mature consideration, and conformably to the fifth article of said constitution, speedily become a part thereof; We the said delegates, in the name, and in [sic] the behalf of the People, of the State of Rhode-Island and Providence-Plantations, do by these Presents, assent to, and ratify the said Constitution. In full confidence . . . That the Congress will not make or alter any regulation in this State, respecting the times, places and manner of holding elections for senators and representatives, unless the legislature of this state shall neglect, or refuse to make laws or regulations for the purpose, or from any circumstance be incapable of making the same; and that [i]n those cases, such power will only be exercised, until the legislature of this State shall make provision in the Premises[.]").

(8) Congress finds that the Framers designed and the ratifying States understood the Elections Clause to serve solely as a protective backstop to ensure the preservation of the Federal Government,

not as a font of limitless power for Congress to wrest control of Federal elections from the States.

(9) This understanding was also reinforced by debate during the first Congress that convened under the Constitution where Representative Aedanus Burke proposed a constitutional amendment to limit the Times, Places and Manner Clause to emergencies. Although the amendment failed, those on both sides of the Burke amendment debate already understood the Elections Clause to limit Federal elections power to emergencies.

(10) History clearly shows that even in the first Congress that convened under the Constitution, it was acknowledged and understood through the debates that ensued over the Elections Clause provision that Congress' control over elections is limited.

(11) Similarly, proponent Representative Smith of South Carolina also believed the original text of the Elections Clause already limited the Federal Government's power over Federal elections to emergencies and so thought there would be no harm in supporting an amendment to make that language express. Annals of Congress 801 (1789) Joseph Gales Edition. *A Century of Lawmaking for a New Nation: U.S. Congressional Documents and Debates, 1774 -*

1875 (loc.gov). So, even the records of the First Congress reflect a recognition of the emergency nature of congressional power over Federal elections.

(12) Similarly, the Supreme Court has supported this understanding. In *Smiley v. Holm*, the Court held that Article 1, Section 4 of the Constitution reserved to the States the primary ''...authority to provide a complete code for congressional elections, not only as to times and places, but in relation to notices, registration, supervision of voting, protection of voters, prevention of fraud and corrupt practices, counting of votes, duties of inspectors and canvassers, and making and publication of election returns; in short, to enact the numerous requirements as to procedure and safeguards which experience shows are necessary in order to enforce the fundamental right involved. And these requirements would be nugatory if they did not have appropriate sanctions in the definition of offenses and punishments. All this is comprised in the subject of 'times, places and manner of holding elections', and involves lawmaking in its essential features and most important aspect.''. *Smiley v. Holm*, 285 U.S. 355, 366 (1932).

(13) This holding is consistent with the understanding of the Elections Clause since the framing of the Constitution. The *Smiley* Court also held that while Congress maintains the authority to ''...supplement these state regulations or [to] substitute its own[]'', such authority remains merely ''a general supervisory power over the whole subject.''. *Id.*

(14) More recently, the Court noted in *Arizona v. Inter-Tribal Council of Ariz., Inc.* that ''[t]his grant of congressional power [that is, the fail-safe provision in the Elections Clause] was the Framers' insurance against the possibility that a State would refuse to provide for the election of representatives to the Federal Congress.''. *Arizona v. Inter-Tribal Council of Arizona, Inc.*, 570 U.S. 1, 7–9 (2013). The Court explained that the Elections Clause ''...imposes [upon the States] the duty...to prescribe the time, place, and manner of electing Representatives and Senators[.]''. *Id.* at 8. And, while, as the Court noted, ''[t]he power of Congress over the 'Times, Places, and Manner' of congressional elections is paramount, and may be exercised at any time, and to any extent which it deems expedient; and so far as it is exercised, and no farther, the reg-

ulations effected supersede those of the State which are inconsistent therewith[]'', *id.* at 9, the *Inter-Tribal* Court explained, quoting extensively from the *Federalist* no. 59, that it was clear that the congressional fail-safe included in the Elections Clause was intended for the sorts of governmental self-preservation discussed here: ''[E]very government ought to contain in itself the means of its own preservation[.]''; ''[A]n exclusive power of regulating elections for the national government, in the hands of the State legislatures, would leave the existence of the Union entirely at their mercy. They could at any moment annihilate it by neglecting to provide for the choice of persons to administer its affairs.''. *Id.* at 8.

(15) It is clear in every respect that the congressional fail-safe described in the Elections Clause vests purely secondary authority over Federal elections in the Federal legislative branch and that the primary authority rests with the States. Congressional authority is intended to be, and as a matter of constitutional fact is, limited to addressing the worst imaginable issues, such as invasion or other matters that might lead to a State not electing representatives to constitute the two Houses of Con-

gress. Congress' authority has never extended to the day-to-day authority over the ''Times, Places and Manner of Election'' that the Constitution clearly reserves to the States.

(16) Congress must act within the bounds of its constitutional authority when enacting legislation concerning the administration of our nation's elections.

Subtitle B—Voluntary Considerations for State Administration of Federal Elections

SEC. 111. SHORT TITLE.

This subtitle may be cited as the ''Voluntarily Offered Tools for Election Reforms by States Act'' or the ''VOTERS Act''.

SEC. 112. FINDINGS.

Congress finds the following:

(1) [*to be provided*]

SEC. 113. ELECTION INTEGRITY VOLUNTARY CONSIDERATIONS.

(a) IN GENERAL.—Subtitle C of title II of the Help America Vote Act of 2002 (52 U.S.C. 20981 et seq.) is amended—

(1) by redesignating section 247 as section 248; and

(2) by inserting after section 246 the following new section:

"SEC. 247. RELEASE OF VOLUNTARY CONSIDERATIONS BY STANDARDS BOARD WITH RESPECT TO ELECTION ADMINISTRATION.

"(a) IN GENERAL.—The Standards Board shall draw from experiences in their home jurisdictions and information voluntarily provided by and between States on what has worked and not worked and release voluntary considerations with respect to the administration of an election for Federal office.

"(b) MATTERS TO CONSIDER.—In releasing the voluntary considerations under subsection (a), the Standards Board shall examine and consolidate information provided by States and release considerations with respect to each of the following categories:

"(1) The process for the administration of ballots delivered by mail, including—

"(A) deadlines for the return and receipt of such ballots to the appropriate election official;

"(B) the design of such ballots, including the envelopes used to deliver the ballots;

"(C) the process for requesting and tracking the return of such ballots; and

"(D) the processing of such ballots upon receipt by the appropriate election official, including the schedule for counting the ballots and the reporting of the unofficial results of such counting.

"(2) The signature verification procedures used to verify the identity of voters in an election, which shall include an evaluation of human and machine methods of signature verification, an assessment of the training provided to individuals tasked to carry out such verification procedures, and the proposal of other less subjective methods of confirming the identity of a voter such as requiring the identification number of a valid government-issued photo identification or the last four digits of the voter's social security number to be provided along with the voter's signature.

"(3) The processes used to carry out maintenance of the official list of persons registered to vote in each State.

"(4) Rules and requirements with respect to the access provided to election observers.

"(5) The processes used to ensure the timely and accurate reporting of the unofficial results of ballot counting in each polling place in a State and the reporting of the unofficial results of such counting.

"(6) The methods used to recruit poll workers and designate the location of polling places during a pandemic, natural disaster, or other emergency.

"(7) The education of the public with respect to the certification and testing of voting machines prior to the use of such machines in an election for Federal office, including education with respect to how such machines are tested for accuracy and logic.

"(8) The processes and procedures used to carry out a post-election audit.

"(9) The processes and procedures used to ensure a secure chain of custody with respect to ballots and election equipment.

"(c) RELEASE OF VOLUNTARY CONSIDERATIONS.—

"(1) DEADLINE FOR RELEASE.—**[***New (conform that this is correct):***]** Not later than 6 months after the date of the enactment of the ACE Act, the Standards Board shall release voluntary considerations with respect to each of the categories described in subsection (b).

"(2) TRANSMISSION AND NOTIFICATION REQUIREMENTS.—Not later than 15 days after the date the Standards Board releases voluntary considerations with respect to a category described in subsection (b), the Commission shall—

"(A) transmit the considerations to the chief State election official of each State and the elected leadership of the legislature of each State, including the elected leadership of any committee of the legislature of a State with jurisdiction with respect to elections;

"(B) make the considerations available on a publicly accessible Government website; and

"(C) notify and transmit the considerations to the chair and ranking minority member of the Committee on House Administration of the House of Representatives and the chair and ranking minority member of the Committee on Rules and Administration of the Senate.

"(d) USE OF REQUIREMENTS PAYMENTS FOR IMPLEMENTATION OF VOLUNTARY CONSIDERATIONS.—A State may use a requirements payment provided under this Act to implement any of the voluntary considerations released under subsection (a).

"(e) RULE OF CONSTRUCTION.—Nothing in this section may be construed—

"(1) to require compliance with the voluntary considerations released under subsection (a), including as a condition of the receipt of Federal funds; or

"(2) ⟦*New:*⟧ to treat the lack of compliance with such considerations as a violation of the Voting Rights Act of 1965 or to treat compliance with such considerations as a defense against an alleged violation of such Act.".

(b) CLERICAL AMENDMENT.—The table of contents of such Act is amended—

(1) by redesignating the item relating to section 247 as relating to section 248; and

(2) by inserting after the item relating to section 246 the following new item:

"Sec. 247. Release of voluntary considerations by Standards Board with respect to election administration.".

Subtitle C—Requirements to Promote Integrity in Election Administration

SEC. 121. ENSURING ONLY ELIGIBLE AMERICAN CITIZENS MAY PARTICIPATE IN FEDERAL ELECTIONS.

(a) SHORT TITLE.—This section may be cited as the "Non-Citizens: Outlawed from Voting in Our Trusted Elections Act of 2022" or the "NO VOTE for Non-Citizens Act of 2022".

(b) FINDINGS; SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) Every eligible person who wishes to cast a ballot in a Federal election must be permitted to do so according to law, and their ballot must be examined according to law, and, if it meets all lawful requirements, counted.

(B) Congress has long required States to maintain Federal voter registration lists in a manner that promotes voter confidence.

(C) The changes included herein are not intended to be an expansion of Federal power but rather a clarification of State authority.

(D) The Fifteenth Amendment, the Nineteenth Amendment, the Twenty-Fourth Amendment, and the Twenty-Sixth Amendment, among other references, make clear that the Constitution prohibits voting by non-citizens in Federal elections.

(E) Congress has the constitutional authority, including under the aforementioned amendments, to pass statutes preventing non-citizens from voting in Federal elections, and did so with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

(F) Congress may further exercise its constitutional authority to ensure the Constitution's prohibition on non-citizen voting in Federal elections is upheld.

(G) Since the Constitution prohibits non-citizens from voting in Federal elections, such ineligible persons must not be permitted to be placed on Federal voter registration lists.

(H) Improper placement of an ineligible non-citizen on a Federal voter registration list leads to—

(i) confusion on the part of the ineligible person with respect to their ineligibility to cast a ballot; and

(ii) an increased likelihood that human error will permit ineligible persons to cast ballots in Federal elections.

(I) State officials have confirmed that poorly maintained voter registration lists lead to ineligible persons casting ballots in Federal elections.

(J) A former Broward County, Florida, elections supervisor has confirmed that ineligible non-voters were able to cast ballots in previous elections and that she was not able to locate as many as 2,040 ballots during the 2018 midterm recount.

(K) This clarification of State authority to maintain Federal voter registration lists to ensure non-citizens are not included on such lists will promote voter confidence in election processes and outcomes.

(L) Congress has the authority to ensure that no Federal elections funding is used to support States that permit non-citizens to cast ballots in any election.

(M) Federal courts and executive agencies have much of the information States may need to maintain their Federal voter registration lists, and those entities should make that information accessible to State election authorities.

(N) It is important to clarify the penalty for any violation of law that allows a non-citizen to cast a ballot in a Federal election.

(O) To protect the confidence of voters in Federal elections, it is important to implement the policy described herein.

(2) SENSE OF CONGRESS.—It is the sense of Congress that—

(A) many States have not adequately met the requirements concerning the removal of ineligible persons from State voter registration rolls pursuant to section 8 of the National Voter Registration Act of 1993 (52 U.S.C. 20507) and should strive to audit and update their voter registration rolls on a routine basis;

(B) allowing non-citizens to cast ballots in American elections weakens our electoral system and the value of citizenship and sows distrust in our elections system;

(C) even if a State has the sovereign authority, no State should permit non-citizens to cast ballots in State or local elections;

(D) States should use all information available to them to maintain Federal voter registration lists and should inform Congress if such data is insufficient; and

(E) Congress may take further action in the future to address this problem.

(c) Clarifying Authority of States to Remove Noncitizens From Voting Rolls.—

(1) Authority under regular removal programs.—Section 8(a)(4) of the National Voter Registration Act of 1993 (52 U.S.C. 20507(a)(4)) is amended—

(A) by striking ‘‘or’’ at the end of subparagraph (A);

(B) by redesignating subparagraph (B) as subparagraph (C); and

(C) by inserting after subparagraph (A) the following new subparagraph:

''(B) the registrant's status as a noncitizen of the United States; or''.

(2) CONFORMING AMENDMENT RELATING TO ONGOING REMOVAL.—Section 8(c)(2)(B)(i) of such Act (52 U.S.C. 20507(c)(2)(B)(i)) is amended by striking ''(4)(A)'' and inserting ''(4)(A) or (B)''.

(d) REQUIREMENT TO MAINTAIN SEPARATE STATE VOTER REGISTRATION LIST FOR NONCITIZENS.—Section 8(a) of the National Voter Registration Act of 1993 (52 U.S.C. 20507(a)) is amended—

(1) in paragraph (5)(B), by striking ''and'' at the end;

(2) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(7) in the case of a State that allows individuals who are not citizens of the United States to vote in elections for public office in the State or any local jurisdiction of the State, ensure that the name of any registrant who is not a citizen of the United

States is maintained on a voter registration list that is separate from the official list of eligible voters with respect to registrants who are citizens of the United States.''.

(e) REQUIREMENTS FOR BALLOTS FOR STATE OR LOCAL JURISDICTIONS THAT ALLOW NONCITIZEN VOTING.—Section 301(a)(1) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(1)) is amended by adding at the end the following new subparagraph:

``(D) In the case of a State or local jurisdiction that allows individuals who are not citizens of the United States to vote in elections for public office in the State or local jurisdiction, the ballot used for the casting of votes by a noncitizen in such State or local jurisdiction may only include the candidates for the elections for public office in the State or local jurisdiction for which the noncitizen is permitted to vote.''.

(f) REDUCTION IN PAYMENTS FOR ELECTION ADMINISTRATION TO STATES OR LOCAL JURISDICTIONS THAT ALLOW NONCITIZEN VOTING.—

(1) IN GENERAL.—Title IX of the Help America Vote Act of 2002 (52 U.S.C. 21141 et seq.) is

amended by adding at the end the following new section:

"SEC. 907. REDUCTION IN PAYMENTS TO STATES OR LOCAL JURISDICTIONS THAT ALLOW NONCITIZEN VOTING.

"(a) IN GENERAL.—Notwithstanding any other provision of this Act, the amount of a payment under this Act to any State or local jurisdiction that allows individuals who are not citizens of the United States to vote in elections for public office in the State or local jurisdiction shall be reduced by 30 percent.

"(b) PROHIBITION ON USE OF FUNDS FOR CERTAIN ELECTION ADMINISTRATION ACTIVITIES.—Notwithstanding any other provision of law, no Federal funds may be used to implement the requirements of section 8(a)(7) of the National Voter Registration Act of 1993 (52 U.S.C. 20507(a)(7)) (as added by section 121(d) of the American Confidence in Elections Act) or section 301(a)(1)(D) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(1)(D)) (as added by section 121(e) of the American Confidence in Elections Act) in a State or local jurisdiction that allows individuals who are not citizens of the United States to vote in elections for public office in the State or local jurisdiction.".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end the following new item:

"Sec. 907. Reduction in payments to States or local jurisdictions that allow noncitizen voting.".

(g) PROMOTING PROVISION OF INFORMATION BY FEDERAL ENTITIES.—

(1) IN GENERAL.—Each entity of the Federal government which maintains information which is relevant to the status of an individual as a registered voter in elections for Federal office in a State shall, upon the request of an election official of the State, provide that information to the election official.

(2) POLICIES AND PROCEDURES.—Consistent with section 3506(g) of title 44, United States Code, an entity of the Federal government shall carry out this subsection in accordance with policies and procedures which will ensure that the information is provided securely, accurately, and in a timely basis.

(3) CONFORMING AMENDMENT RELATING TO COVERAGE UNDER PRIVACY ACT.—Section 552a(b) of title 5, United States Code, is amended—

(A) by striking "or" at the end of paragraph (11);

(B) by striking the period at the end of paragraph (12) and inserting "; or"; and

(C) by adding at the end the following new paragraph:

"(13) to an election official of a State in accordance with section 121(h) of the American Confidence in Elections Act.".

(h) ENSURING PROVISION OF INFORMATION TO STATE ELECTION OFFICIALS ON INDIVIDUALS RECUSED FROM JURY SERVICE ON GROUNDS OF NONCITIZENSHIP.—

(1) REQUIREMENT DESCRIBED.—If a United States district court recuses an individual from serving on a jury on the grounds that the individual is not a citizen of the United States, the court shall transmit a notice of the individual's recusal—

(A) to the chief State election official of the State in which the individual resides; and

(B) to the Attorney General.

(2) DEFINITIONS.—For purposes of this subsection—

(A) the "chief State election official" of a State is the individual designated by the State under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509) to be responsible for coordination of the State's responsibilities under such Act; and

(B) the term "State" means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, Guam, the United States Virgin Islands, and the Commonwealth of the Northern Mariana Islands.

(i) PROHIBITION ON VOTING BY NONCITIZENS IN FEDERAL ELECTIONS.—

(1) IN GENERAL.—Section 12 of the National Voter Registration Act of 1993 (52 U.S.C. 20511) is amended—

(A) by striking "A person" and inserting "(a) IN GENERAL.—A person"; and

(B) by adding at the end the following new subsection:

"(b) PROHIBITION ON VOTING BY ALIENS.—

"(1) IN GENERAL.—It shall be unlawful for any alien to vote in any election in violation of section 611 of title 18, United States Code.

"(2) PENALTIES.—Any person who violates this subsection shall be fined under title 18, United States Code, imprisoned not more than one year, or both.".

(2) EFFECTIVE DATE.—This subsection and the amendments made by this subsection shall apply

with respect to elections held on or after the date of the enactment of this Act.

SEC. 122. STATE REPORTING REQUIREMENTS WITH RESPECT TO VOTER LIST MAINTENANCE.

Section 8 of the National Voter Registration Act of 1993 (52 U.S.C. 20507) is amended—

(1) in subsection (i), by adding at the end the following:

"(3) The records maintained pursuant to paragraph (1) shall include lists of the names and addresses of all registrants in a State who were inactive according to the criteria described in subsection (d)(1)(B) and the length of time each such registrant has been inactive according to such criteria.";

(2) by redesignating subsection (j) as subsection (k); and

(3) by inserting after subsection (i) the following new subsection:

"(j) REPORTING REQUIREMENTS.—Not later than June 30 of each odd-numbered year, each State shall submit to the Election Assistance Commission a report that includes, with respect to such State during the preceding 2-year period, the total number of—

"(1) registrants who were inactive according to the criteria described in subsection (d)(1)(B) and the length of time each such registrant has been inactive according to such criteria;

"(2) registrants who voted in at least one of the prior 2 consecutive general elections for Federal office;

"(3) registrants removed from the list of official voters in the State pursuant to subsection (d)(1)(B);

"(4) notices sent to registrants pursuant to subsection (d)(2); and

"(5) registrants who received a notice described in paragraph (4) who responded to such notice.".

SEC. 123. CONTENTS OF STATE MAIL VOTER REGISTRATION FORM.

(a) SHORT TITLE.—This section may be cited as the "State Instruction Inclusion Act".

(b) IN GENERAL.—Section 6(a) of the National Voter Registration Act of 1993 (52 U.S.C. 20505(a)) is amended—

(1) in paragraph (1), by inserting ", except that a State may, in addition to the criteria stated in section 9(b), require that an applicant provide proof that the applicant is a citizen of the United States" after "elections for Federal office"; and

(2) in paragraph (2), by inserting "and such form may include a requirement that the applicant

provide proof that the applicant is a citizen of the United States'' after ''elections for Federal office''.

SEC. 124. PROVISION OF PHOTOGRAPHIC CITIZEN VOTER IDENTIFICATION TOOLS FOR STATE USE.

(a) SHORT TITLE.—This section may be cited as the ''Citizen Vote Protection Act''.

(b) FINDINGS; SENSE OF CONGRESS.—

(1) FINDINGS.—Congress finds the following:

(A) Photo voter identification programs established by the States should be administered without unlawful discrimination and with an eye toward balancing appropriate access to the ballot box with election integrity and voter confidence goals.

(B) As confirmed by the bipartisan Commission on Federal Election Reform (commonly known as the Carter-Baker Commission), ''[v]oters in nearly 100 democracies use a photo identification card without fear of infringement of their rights''.

(C) As confirmed by the Carter-Baker Commission, ''[t]he right to vote is a vital component of U.S. citizenship and all States should use their best efforts to obtain proof of citizenship before registering voters.''.

(D) The Carter-Baker Commission was correct in its 2005 report when it recommended that the REAL ID Act be ‘‘modestly adapted for voting purposes to indicate on the front or back whether the individual is a U.S. citizen.’’.

(E) Congress acknowledges the important work completed by the Carter-Baker Commission and, by amending the REAL ID Act, resolves the concerns in the Commission’s report that ‘‘[t]he REAL ID Act does not require that the card indicates citizenship, but that would need to be done if the card is to be used for voting purposes’’.

(F) Photographic voter identification is important for ensuring voter confidence in election processes and outcomes.

(G) Requiring photographic voter identification is well within States’ constitutional competence, including pursuant to the Qualifications Clause of the Constitution of the United States (article I, section 2, clause 2), the Presidential Electors Clause of the Constitution (article II, section 1, clause 2), and the Seventeenth Amendment.

(H) The Fifteenth Amendment, the Nineteenth Amendment, the Twenty-Fourth Amendment, and the Twenty-Sixth Amendment, among other references, make clear that the Constitution prohibits voting by non-citizens in Federal elections.

(I) Congress has the constitutional authority, including under the aforementioned amendments, to pass statutes preventing non-citizens from voting in Federal elections, and did so with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

(J) Congress may further exercise its constitutional authority to ensure the Constitution's prohibition on non-citizen voting in Federal elections is upheld.

(2) SENSE OF CONGRESS.—It is the sense of Congress that the States should implement the substance of the recommendation of the Carter-Baker Commission that, "[t]o ensure that persons presenting themselves at the polling place are the ones on the registration list, the Commission recommends that states [encourage] voters to use the REAL ID card, which was mandated in a law signed by the President in May 2005".

(c) REAL ID ACT AMENDMENT.—

(1) AMENDMENT.—Section 202(b) of the Real ID Act of 2005 (49 U.S.C. 30301 note) is amended by adding at the end the following new paragraph:

"(10) If the person is a citizen of the United States, an indication of that citizenship, except that no other information may be included with respect to the immigration status of the person.".

(2) APPLICABILITY.—The amendment made by this subsection shall be effective January 1, 2026, and shall apply with respect to any driver's license or identification card issued by a State on and after such date.

(d) RULE OF CONSTRUCTION.—Nothing in this section or in any amendment made by this section may be construed to establish or mandate the use of a national identification card or to authorize any office of the executive branch to establish or mandate the use of a national identification card.

SEC. 125. MANDATORY PROVISION OF IDENTIFICATION FOR CERTAIN VOTERS NOT VOTING IN PERSON.

(a) REQUIRING VOTERS TO PROVIDE IDENTIFICATION.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended—

(1) by redesignating sections 304 and 305 as sections 305 and 306; and

(2) by inserting after section 303 the following new section:

"SEC. 304. MANDATORY PROVISION OF IDENTIFICATION FOR CERTAIN VOTERS WHO VOTE BY MAIL.

"(a) FINDING OF CONSTITUTIONAL AUTHORITY.—Congress finds that it has the authority to establish the terms and conditions that States must follow with respect to the administration of voting by mail because article I, section 8, clause 7 of the Constitution of the United States and other enumerated powers grant Congress the power to regulate the operations of the United States Postal Service.

"(b) REQUIRING PROVISION OF IDENTIFICATION TO RECEIVE A BALLOT OR VOTE IN CERTAIN CASES.—

"(1) INDIVIDUALS REQUESTING A BALLOT TO VOTE BY MAIL.—Notwithstanding any other provision of law, the appropriate State or local election official may not provide an individual a ballot to vote by mail for an election for Federal office in a case in which the individual requested such ballot other than in person from the appropriate State or local election official of the State at a State designated elections office unless the individual submits with the application for the ballot a copy of an identification described in paragraph (3).

"(2) INDIVIDUALS VOTING BY MAIL IN CERTAIN CASES.—

"(A) IN GENERAL.—Notwithstanding any other provision of law, in a case in which the appropriate State or local election official provides an individual a ballot to vote by mail for an election for Federal office without requiring such individual to submit a separate application or request to receive such ballot for each such election, the election official may not accept the voted ballot unless the individual submits with the voted ballot a copy of an identification described in paragraph (3).

"(B) FAIL-SAFE VOTING.—An individual who desires to vote other than in person but who does not meet the requirements of subparagraph (A) may cast such a ballot other than in person and the ballot shall be counted as a provisional ballot in accordance with section 302(a).

"(3) IDENTIFICATION DESCRIBED.—An identification described in this paragraph is, with respect to an individual—

"(A) a current and valid photo identification of the individual;

"(B) a copy of a current utility bill, bank statement, government check, paycheck, or other government document that shows the name and address of the individual;

"(C) a valid driver's license or an identification card issued by a State or the identification number for such driver's license or identification card issued by a State;

"(D) the last 4 digits of the individual's social security number; or

"(E) such other documentation issued by a Federal, State, or local government that provides the same or more identifying information as required by subparagraphs (A) through (D) such that the election official is reasonably certain as to the identity of the individual.

"(c) EXCEPTIONS.—This section does not apply with respect to any individual who is—

"(1) entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.);

"(2) provided the right to vote otherwise than in person under section 3(b)(2)(B)(ii) of the Voting

Accessibility for the Elderly and Handicapped Act (52 U.S.C. 20102(b)(2)(B)(ii)); or

"(3) entitled to vote otherwise than in person under any other Federal law.

"(d) RULE OF CONSTRUCTION.—Nothing in this section may be construed as prohibiting a State from imposing identification requirements to request a ballot to vote by mail or cast a vote by mail that are more stringent than the requirements under this section.

"(e) EFFECTIVE DATE.—This section shall take effect on January 1, 2024.".

(b) CONFORMING AMENDMENTS RELATING TO EXISTING IDENTIFICATION REQUIREMENTS.—

(1) TREATMENT AS INDIVIDUALS REGISTERING TO VOTE BY MAIL FOR PURPOSES OF FIRST-TIME VOTER IDENTIFICATION REQUIREMENTS.—Section 303(b)(1)(A) of the Help America Vote Act of 2002 (52 U.S.C. 21083(b)(1)(A)) is amended by striking "by mail" and inserting "by mail or otherwise not in person at an elections office or voter registration agency of the State".

(2) EXCEPTIONS.—Section 303(b)(3) of the Help America Vote Act of 2002 (52 U.S.C. 21083(b)(3)) is amended—

(A) in subparagraph (A), by striking "by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4)" and inserting "by mail under section 6 of the National Voter Registration Act of 1993 (52 U.S.C. 20505) or otherwise not in person at a voter registration agency of the State"; and

(B) in subparagraph (B)(i), by striking "by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4)" and inserting "by mail under section 6 of the National Voter Registration Act of 1993 (52 U.S.C. 20505) or otherwise not in person at a voter registration agency of the State".

(3) EXPANSION OF TYPES OF IDENTIFICATION PERMITTED.—Section 303(b)(2)(A) of the Help America Vote Act of 2002 (52 U.S.C. 21083(b)(2)(A)) is amended—

(A) in clause (i)—

(i) in subclause (I), by striking "or" at the end; and

(ii) by adding at the end the following new subclause:

"(III) such other documentation issued by a Federal, State, or local government that provides the same or more identifying information as required by subclauses (I) and (II) such that the election official is reasonably certain as to the identity of the individual; or''; and

(B) in clause (ii)—

(i) in subclause (I), by striking ''or'' at the end;

(ii) in subclause (II), by striking the period at the end and inserting ''; or''; and

(iii) by adding at the end the following new subclause:

''(III) such other documentation issued by a Federal, State, or local government that provides the same or more identifying information as required by subclauses (I) and (II) such that the election official is reasonably certain as to the identity of the individual.''.

(c) CONFORMING AMENDMENT RELATING TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking ''and 303'' and inserting ''303, and 304''.

(d) CLERICAL AMENDMENT.—The table of contents of such Act is amended—

(1) by redesignating the items relating to sections 304 and 305 as relating to sections 305 and 306; and

(2) by inserting after the item relating to section 303 the following:

"Sec. 304. Mandatory provision of identification for certain voters who vote by mail.".

SEC. 126. CONFIRMING ACCESS FOR CONGRESSIONAL ELECTION OBSERVERS.

(a) SHORT TITLE.—This section may be cited as the "Confirmation of Congressional Observer Access Act of 2022" or the "COCOA Act of 2022".

(b) FINDINGS RELATING TO CONGRESSIONAL ELECTION OBSERVERS.—Congress finds the following:

(1) The Constitution delegates to each of House of the Congress the authority to "be the Judge of the Elections, Returns and Qualifications of its own Members".

(2) While, in general, Congress shall respect the determination of State authorities with respect to the election of members to each House, each House of Congress serves as the final arbiter over any contest to the seating of any putative Member-elect or Senator-elect.

(3) These election contest procedures are contained in the precedents of each House of Congress. Further, for the House of Representatives the procedures exist under the Federal Contested Elections Act.

(4) In the post-Civil War modern era, more than 100 election contests have been filed with the House of Representatives.

(5) For decades, Congress has appointed and sent out official congressional observers to watch the administration of congressional elections in the States and territories.

(6) These observers serve to permit Congress to develop its own factual record in preparation for eventual contests and for other reasons.

(7) This section and the amendments made by this section do not establish any new authorities or procedures but are provided simply to permit a convenient statutory reference for existing Congressional authority and activity.

(c) CONFIRMING REQUIREMENT THAT STATES PROVIDE ACCESS.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.), as amended by section 125(a), is amended—

(1) by redesignating sections 305 and 306 as sections 306 and 307; and

(2) by inserting after section 304 the following new section:

"SEC. 305. CONFIRMING ACCESS FOR CONGRESSIONAL ELECTION OBSERVERS.

"(a) FINDING OF CONSTITUTIONAL AUTHORITY.—Congress finds that it has the authority to require that States allow access to designated Congressional election observers to observe the election administration procedures in an election for Federal office because the authority granted to Congress under article I, section 5 of the Constitution of the United States gives each House of Congress the power to be the judge of the elections, returns and qualifications of its own Members.

"(b) REQUIRING STATES TO PROVIDE ACCESS.—A State shall provide each individual who is a designated Congressional election observer for an election with full access to clearly observe all of the elements of the administration procedures with respect to such election, including but not limited to in all areas of polling places and other facilities where ballots in the election are processed, tabulated, cast, canvassed, and certified, in all areas where voter registration activities occur before such election, and in any other such place where election administration procedures to prepare for the election or carry out any post-election recounts take place. No designated Congressional election observer may handle ballots, elections equipment (voting or non-voting), advocate for a position or candidate, take any action to reduce ballot secrecy, or otherwise interfere with the elections administration process.

"(c) DESIGNATED CONGRESSIONAL ELECTION OBSERVER DESCRIBED.—In this section, a 'designated Congressional election observer' is an individual who is designated in writing by the chair or ranking minority member of the Committee on House Administration of the House of Representatives or the Committee on Rules and Administration of the Senate, or the successor committee in either House of Congress to gather information with respect to an election, including in the event that the election is contested in the House of Representatives or the Senate and for other purposes permitted by article 1, section 5 of the Constitution of the United States.".

(d) CONFORMING AMENDMENT RELATING TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111), as amended by section 125(c), is amended by striking "and 304" and inserting "304, and 305".

(e) CLERICAL AMENDMENT.—The table of contents of such Act, as amended by section 125(d), is amended—

(1) by redesignating the items relating to sections 305 and 306 as relating to sections 306 and 307; and

(2) by inserting after the item relating to section 304 the following:

"Sec. 305. Confirming access for Congressional election observers.".

SEC. 127. USE OF REQUIREMENTS PAYMENTS FOR POST-ELECTION AUDITS.

Section 251(b)(1) of the Help America Vote Act of 2002 (52 U.S.C. 21001(b)(1)) is amended by inserting ", including to conduct and publish an audit of the effectiveness and accuracy of the voting systems, election procedures, and outcomes used to carry out an election for Federal office in the State and the performance of the State and local election officials who carried out the election" after "requirements of title III".

SEC. 128. CERTAIN TAX BENEFITS AND SIMPLIFICATION WITH RESPECT TO ELECTION WORKERS.

(a) SHORT TITLE.—This section may be cited as the "Election Worker Employer Participation Act".

(b) EXCLUSION FROM GROSS INCOME FOR CERTAIN ELECTION WORKER COMPENSATION.—

(1) IN GENERAL.—Part III of subchapter B of chapter 1 of the Internal Revenue Code of 1986 is amended by inserting after section 139H the following new section:

"SEC. 139I. CERTAIN COMPENSATION OF ELECTION WORKERS.

"(a) IN GENERAL.—Gross income shall not include qualified election worker compensation.

"(b) LIMITATION.—The amount excludible from gross income under subsection (a) with respect to any taxpayer for any taxable year shall not exceed the dollar amount in effect under section 3121(b)(7)(F)(iv) for the calendar year in which such taxable year begins.

"(c) QUALIFIED ELECTION WORKER COMPENSATION.—For purposes of this section, the term 'qualified election worker compensation' means amounts otherwise includible in gross income which are paid by a State, political subdivision of a State, or any instrumentality of a State or any political subdivision thereof, for the service of an individual as an election official or election worker (within the meaning of section 3121(b)(7)(F)(iv)).".

(2) CLERICAL AMENDMENT.—The table of sections for part III of subchapter B of chapter 1 of such Code is amended by inserting after the item relating to section 139H the following new item:

"Sec. 139I. Certain compensation of election workers.".

(c) INFORMATION REPORTING NOT REQUIRED BY REASON OF CERTAIN AMOUNTS EXCLUDIBLE FROM GROSS INCOME.—Section 6041 of such Code is amended by adding at the end the following new subsection:

"(h) TREATMENT OF CERTAIN EXCLUDIBLE COMPENSATION OF ELECTION WORKERS.—In the case of any payment by a State, political subdivision of a State, or any instrumentality of a State or any political subdivision thereof, for the service of an individual as an election official or election worker (within the meaning of section 3121(b)(7)(F)(iv)), the determination of whether the $600 threshold described in subsection (a) has been met with respect to such individual shall be determined by not taking into account—

"(1) any such payment which is qualified election worker compensation (as defined in section 139I(c)) which does not exceed the limitation described in section 139I(b), and

"(2) any such payment which is excludible from the gross income of such individual under section 127.".

(d) EFFECTIVE DATE.—The amendments made by this section shall apply to payments made after December 31, 2022, in taxable years ending after such date.

SEC. 129. VOLUNTARY GUIDELINES WITH RESPECT TO NON-VOTING ELECTION TECHNOLOGY.

(a) SHORT TITLE.—This section may be cited as the "Protect American Voters Act".

(b) ADOPTION OF VOLUNTARY GUIDELINES BY ELECTION ASSISTANCE COMMISSION.—

(1) ADOPTION OF GUIDELINES.—Title II of the Help America Vote Act of 2002 (52 U.S.C. 20921 et seq.) is amended by adding at the end the following new subtitle:

"Subtitle E—Voluntary Guidelines for Use of Nonvoting Election Technology

"SEC. 298. ADOPTION OF VOLUNTARY GUIDELINES BY COMMISSION.

''(a) ADOPTION.—The Commission shall adopt voluntary guidelines for election officials on the use of nonvoting election technology, taking into account the recommendations of the Standards Board ⟦*New:*⟧ and the Local Leadership Council of the Commission under section 298A.

''(b) REVIEW.—The Commission shall review the guidelines adopted under this subtitle not less frequently than once every 4 years, and may adopt revisions to the guidelines as it considers appropriate.

''(c) PROCESS FOR ADOPTION.—The adoption of the voluntary guidelines under this subtitle shall be carried out by the Commission in a manner that provides for each of the following:

"(1) Publication of notice of the proposed guidelines in the Federal Register.

"(2) An opportunity for public comment on the proposed guidelines.

"(3) An opportunity for a public hearing on the record.

"(4) Publication of the final recommendations in the Federal Register.

"(d) DEADLINE FOR INITIAL SET OF GUIDELINES.—The Commission shall adopt the initial set of voluntary guidelines under this section not later than December 31, 2025.

"SEC. 298A. ROLE OF STANDARDS BOARD AND LOCAL LEADERSHIP COUNCIL.

"(a) DUTIES.—The Standards Board ⟦New:⟧ and the Local Leadership Council of the Commission shall assist the Commission in the adoption of voluntary guidelines under section 298, including by providing the Commission with recommendations on appropriate standards for the use of nonvoting election technology, including standards to ensure the security and accuracy, and promote the usability, of such technology, and by conducting a review of existing State programs with respect to the testing of nonvoting election technology.

"(b) SOURCES OF ASSISTANCE.—

"(1) CERTAIN MEMBERS OF TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.—The following members of the Technical Guidelines Development Committee under section 221 shall assist the Standards Board ⟦*New:*⟧ and the Local Leadership Council in carrying out their duties under this section:

"(A) The Director of the National Institute of Standards and Technology.

"(B) The representative of the American National Standards Institute.

"(C) The representative of the Institute of Electrical and Electronics Engineers.

"(D) The 4 members of the Technical Guidelines Development Committee appointed under subsection (c)(1)(E) of such section as the other individuals with technical and scientific expertise relating to voting systems and voting equipment.

"(2) DETAILEE FROM CISA.—The Executive Board of the Standards Board may request the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to provide a detailee to assist the Standards Board in carrying out its duties under this section, so long as such detailee has no involvement in the drafting of any of the voluntary guidelines.

"SEC. 298B. USE OF PAYMENTS TO OBTAIN OR UPGRADE TECHNOLOGY.

"A State may use funds provided under any law for activities to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements, to obtain nonvoting election technology which is in compliance with the voluntary guidelines adopted under section 298 or to upgrade nonvoting election technology so that the technology is in compliance with such guidelines, and may, notwithstanding any other provision of law, use any unobligated grant funding provided to the State by the Election Assistance Commission from amounts appropriated under the heading 'Independent Agencies—Election Assistance Commission—Election Security Grants' in title V of division C of the Consolidated Appropriations Act, 2020 (Public Law 116–93) for the purposes of enhancing election technology and making election security improvements until December 31, 2024.

"SEC. 298C. NONVOTING ELECTION TECHNOLOGY DEFINED.

"In this subtitle, the term 'nonvoting election technology' means technology used in the administration of elections for Federal office which is not used directly in the casting, counting, tabulating, or collecting of ballots or votes, including each of the following:

"(1) Electronic pollbooks or other systems used to check in voters at a polling place or verify a voter's identification.

"(2) Election result reporting systems.

"(3) Electronic ballot delivery systems.

"(4) Online voter registration systems.

"(5) Polling place location search systems.

"(6) Sample ballot portals.

"(7) Signature systems.

"(8) Such other technology as may be recommended for treatment as nonvoting election technology as the Standards Board may recommend.".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end of the items relating to title II the following:

"Subtitle E—Voluntary Guidelines for Use of Nonvoting Election Technology

"Sec. 298. Adoption of voluntary guidelines by Commission.
"Sec. 298A. Role of Standards Board and Local Leadership Council.
"Sec. 298B. Use of payments to obtain or upgrade technology.
"Sec. 298C. Nonvoting election technology defined.".

(c) TREATMENT OF TECHNOLOGY USED IN MOST RECENT ELECTION.—Any nonvoting election technology, as defined in section 298C of the Help America Vote Act of 2002 (as added by subsection (a)(1)), which a State used in the most recent election for Federal office held in the State prior to the date of the enactment of this Act shall be deemed to be in compliance with the voluntary guidelines on the use of such technology which are adopted by the Election Assistance Commission under section 298 of such Act (as added by subsection (a)(1)).

SEC. 130. STATUS REPORTS BY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.

Section 231 of the Help America Vote Act of 2002 (52 U.S.C. 20971) is amended by adding at the end the following new subsection:

"(e) STATUS REPORTS BY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—Not later than 60 days after the end of each fiscal year (beginning with 2023), the Director of the National Institute of Standards and Technology shall submit to Congress a status report describing—

"(1) the extent to which the Director carried out the Director's responsibilities under this Act during the fiscal year, including the responsibilities imposed under this section and the responsibilities imposed with respect to the Technical Guidelines Development Committee under section 222, together with the Director's best estimate of when the Director will completely carry out any responsibility which was not carried out completely during the fiscal year; and

"(2) the extent to which the Director carried out any projects requested by the Commission during the fiscal year, together with the Director's best estimate of when the Director will complete any such project which the Director did not complete during the fiscal year.".

SEC. 131. 501(c)(3) ORGANIZATIONS PROHIBITED FROM PROVIDING DIRECT FUNDING TO ELECTION ORGANIZATIONS.

(a) IN GENERAL.—Section 501(c)(3) of the Internal Revenue Code of 1986 is amended—⟦*New (based on HR 1725): Note that, as drafted, this would not only prohibit any 501(c)(3) organization from providing any form of assistance with respect to the administration of an election (e.g., a church couldn't permit its building be used as a polling place), but that, read technically, this language would prohibit any 501(c)(3) organization from providing anything of value to a State or local government for any reason whatsoever, even if it has nothing to do with the administration of an election (including providing scholarships to local schools, remodeling parks and recreation facilities, or giving local law enforcement a discount on equipment and services).*⟧

(1) by striking "and which does not participate" and inserting "which does not participate", and

(2) by striking the period at the end and inserting ", and which does not provide below-cost services, scholarships, subsidies, or direct, in-kind, or indirect funding to official election organizations, including any State or local government entity or any government election organization.".

(b) EFFECTIVE DATE.—The amendments made by this section shall apply to funding provided in taxable years beginning after December 31, 2023.

SEC. 132. REQUIREMENTS WITH RESPECT TO ELECTION MAIL.

(a) SHORT TITLE.—This section may be cited as the "Election Integrity Mail Reform Act of 2022".

(b) PRIORITIZING ELECTION MAIL.—Title 39, United States Code, is amended by adding after chapter 36 the following:

"CHAPTER 37—ELECTION AND POLITICAL MAIL

"§ 3701. Prioritization of processing and delivery of election mail

"(a) IN GENERAL.—The Postal Service shall give priority to the processing and delivery of election mail. In carrying out this subsection, the Postal Service shall at a minimum—

"(1) deliver any election mail regardless of the amount of postage paid;

"(2) shall, to the greatest extent practicable, process and clear election mail from any postal facility each day; and

"(3) carry and deliver election mail expeditiously.

"(b) ELECTION MAIL WITH INSUFFICIENT POSTAGE.—In carrying out subsection (a)(1), the Postal Service shall process and deliver election mail with insufficient postage in the same manner as election mail with sufficient postage, but may collect insufficient postage after delivery of any election mail with insufficient postage.

"(c) UNDERFUNDED OR OVERDRAWN ACCOUNTS.—The Postal Service shall process and deliver election mail, under the standards in place under subsection (a), sent from a customer using an account registered with the Postal Service (including a corporate account or an advance deposit account) even if such account is underfunded or overdrawn. Nothing in this section shall be construed to limit or otherwise prevent the Postal Service from seeking reimbursement from any person regarding unpaid postage.

"(d) ELECTION MAIL DEFINED.—In this chapter, the term 'election mail' means any item mailed to or from an individual for purposes of the individual's participation in an election for public office, including balloting materials, voter registration cards, absentee ballot applications, polling place notification and photographic voter identification materials.

"§ 3702. Use of nonprofit permit for cooperative mailings

"Notwithstanding any other law, rule, or regulation, a national, State, or local committee of a political party (as defined under the Federal Election Campaign Act of 1971) which is eligible to mail at the nonprofit rate may conduct a cooperative mailing at that nonprofit rate with a candidate, a candidate's committee, or another committee of a political party, and may seek reimbursement from such a candidate, candidate's committee, or committee of a political party for the costs of such mailing.

"§ 3703. Marking or notice on election mail

"(a) IN GENERAL.—For the purposes of assisting election officials in processing election mail, the Postal

Service shall place a marking or notice indicating that a piece of mail is election mail.

"(b) REQUIREMENTS.—The Postal Service may determine the appropriate manner in which subsection (a) is carried out, but at a minimum such marking or notice shall—

"(1) be placed, as soon as practicable, at the time the election mail is received by the Postal Service, in a conspicuous and legible type or in a common machine-readable technology on the envelope or other cover in which the election mail is mailed; and

"(2) clearly demonstrate the date and time that such marking or noticed was so placed.

"(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed as requiring any change to the processes and procedures used by the Postal Service with respect to Postal Service barcodes on envelopes carried or delivered by the Postal Service.

"§ 3704. Application to Uniformed and Overseas Citizens Absentee Voting Act

"This chapter shall not apply to balloting materials under the Uniformed and Overseas Citizens Absentee Voting Act and nothing in this chapter shall be construed to alter or otherwise affect the operation of such Act or section 3406 of this title.".

(c) POSTMARKING STAMPS.—Section 503 of title 18, United States Code, is amended—

(1) by striking ''Whoever forges'' and inserting ''(a) Whoever forges'';

(2) by striking ''or such impression thereof,'' and all that follows and inserting the following: ''or such impression thereof—

''(1) shall be fined under this title or imprisoned not more than five years, or both; or

''(2) if the impression from a postmarking stamp or impression thereof forged, counterfeited, used, sold, or possessed in violation of this section is applied to a mailed ballot for an election for Federal, State, or local office, shall be fined under this title or imprisoned not more than 10 years, or both.''; and

(3) by adding at the end following new subsection:

''(a) Whoever, with the intent to falsify the date on which a postmark was applied, applies to a mailed ballot described in subsection (a)(2) a genuine postmark that bears a date other than the date on which such postmark was applied, shall be subject to the penalties set forth in such subsection.''.

SEC. 133. CLARIFICATION OF RIGHT OF STATE TO APPEAL DECISIONS THROUGH DULY AUTHORIZED REPRESENTATIVE.

Section 1254 of title 28, United States Code, is amended—

(1) in paragraph (1), by striking the semicolon at the end and inserting a period; and

(2) by adding at the end the following:

"(3) By appeal by a party (including the State as represented by any agent authorized as a party under State law) relying on a State statute held by a court of appeals to be invalid as repugnant to the Constitution, treaties or laws of the United States, but such appeal shall preclude review by writ of certiorari at the instance of such appellant, and the review on appeal shall be restricted to the Federal questions presented.".

SEC. 134. FEDERAL AGENCY INVOLVEMENT IN VOTER REGISTRATION ACTIVITIES.

(a) SHORT TITLE.—This section may be cited as the "Promoting Free and Fair Elections Act". [*Note: Subsections (a), (c), (d), (e), and (f) are from HR 3072, while subsection (b) is the text of section 134 of the ACE Act from the 117th.*]

(b) CLARIFICATION OF FEDERAL AGENCY INVOLVEMENT IN VOTER REGISTRATION ACTIVITIES.—Executive

Order 14019 (86 Fed. Reg. 13623; relating to promoting access to voting) shall have no force or effect to the extent that it is inconsistent with section 7 of the National Voter Registration Act of 1993 (52 U.S.C. 20506).

(c) PROHIBITING PROMOTION OF VOTER REGISTRATION BY AGENCIES.—

(1) AGREEMENTS WITH NONGOVERNMENTAL ORGANIZATIONS.—None of the funds made available for the salaries and expenses of an agency may be used to solicit or enter into an agreement with a nongovernmental organization to conduct voter registration or voter mobilization activities, including registering voters or providing any person with voter registration materials, absentee or vote-by-mail ballot applications, voting instructions, or candidate-related information, on the property or website of the agency.

(2) ACTIVITIES UNDER EXECUTIVE ORDER 14019.—

(A) DELAY IN IMPLEMENTATION.—

(i) DELAY.—Except as provided in clause (ii), none of the funds made available for the salaries and expenses of an agency may be used to implement activities directed under Executive Order 14019 (86 Fed. Reg. 13623) until—

(I) in the case of an agency that is required to submit a report to the appropriate congressional committees under subparagraph (B)(i), 180 days after the agency submits the report; or

(II) in the case of an agency that is required to submit a report to the appropriate congressional committees under subparagraph (B)(ii), the date on which the agency submits the report.

(ii) EXCEPTION.—Clause (i) shall not apply to any activity described in section 7(c) of the National Voter Registration Act of 1993 (52 U.S.C. 20506(c)).

(B) REPORT.—Not later than 30 days after the date of enactment of this Act, the head of each agency shall submit to the appropriate congressional committees—

(i) a copy of the strategic plan of the agency for promoting voter registration and voter participation under section 3(b) of Executive Order 14019 (86 Fed. Reg. 13623) that the agency developed or submitted to the Assistant to the President for Domestic Policy; or

(ii) if the agency did not develop or submit a plan described in clause (i) to the Assistant to the President for Domestic Policy, a certification signed by the head of the agency that the agency did not develop or submit such a plan.

(3) EFFECTIVE DATE.—Except as provided in paragraph (2)(B), this section shall apply with respect to fiscal year 2023 and each succeeding fiscal year.

(d) ADDITIONAL REPORT ON VOTER REGISTRATION AND MOBILIZATION.—Not later than 30 days after the date of enactment of this Act, the head of each agency shall submit to the appropriate congressional committees a report describing the activities carried out by the agency pursuant to sections 3 and 4 of Executive Order 14019 (86 Fed. Reg. 13623).

(e) PROHIBITING VOTER REGISTRATION AND MOBILIZATION IN FEDERAL WORK-STUDY PROGRAMS.—Section 443(b)(1) of the Higher Education Act of 1965 (20 U.S.C. 1087–53(b)(1)) is amended—

(1) in subparagraph (C), by striking ''and'';

(2) by redesignating subparagraph (D) as subparagraph (E); and

(3) by inserting after subparagraph (C) the following:

''(D) does not involve registering or mobilizing voters on or off the campus of the institution; and''.

(f) DEFINITIONS.—In this section:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502(1) of title 44, United States Code, except that for purposes of subsection (c)(2) such term does not include an independent regulatory agency as defined in section 3502(5) of title 44, United States Code.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Rules and Administration of the Senate;

(B) the Committee on the Judiciary of the Senate;

(C) the Committee on House Administration of the House of Representatives; and

(D) the Committee on the Judiciary of the House of Representatives.

SEC. 135. PROHIBITION ON USE OF FEDERAL FUNDS FOR ELECTION ADMINISTRATION IN STATES THAT PERMIT BALLOT HARVESTING.

(a) SHORT TITLE.—This section may be cited as the ''No Federal Funds for Ballot Harvesting Act''.

(b) FINDINGS.—Congress finds that—

(1) the right to vote is a fundamental right of citizens of the United States, as described by the Constitution of the United States;

(2) the Committee on House Administration of the House of Representatives, which is charged with investigating election irregularities, received reports through its official Election Observer Program for the 2018 general election and the 2020 general election, as well as from other stakeholders, that individuals other than voters themselves were depositing large amounts of absentee ballots at polling places throughout California and other States, a practice colloquially known as ''ballot harvesting'';

(3) the practice of ballot harvesting creates significant vulnerabilities in the chain-of-custody of ballots because individuals collecting ballots are not required to be registered voters and are not required

to identify themselves at a voter's home, and the State does not track how many ballots are harvested in an election;

(4) in North Carolina, a congressional election was invalidated due to fraud associated with ballot harvesting committed by a political operative, and it is unlikely such activity would have been detected were it not for the prohibition against ballot harvesting in the State;

(5) ballot harvesting invites electioneering activity at home and weakens States' long-standing voter protection procedures, which remain in place at polling locations, creating the possibility of undue influence over voters by political operatives and other bad actors; and

(6) the Supreme Court of the United States has affirmed State authority to restrict ballot harvesting (*Brnovich v. Democratic National Committee*, 141 S. Ct. 2321 (2021)).

(c) PROHIBITION ON FEDERAL FUNDS FOR ELECTION ADMINISTRATION FOR STATES ALLOWING COLLECTION AND TRANSMISSION OF BALLOTS BY CERTAIN THIRD PARTIES.—

(1) IN GENERAL.—The Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.) is amended by adding at the end the following new section:

"SEC. 908. PROHIBITION ON FEDERAL FUNDS FOR ELECTION ADMINISTRATION FOR STATES ALLOWING COLLECTION AND TRANSMISSION OF BALLOTS BY CERTAIN THIRD PARTIES.

"(a) IN GENERAL.—Notwithstanding any other provision of law, no Federal funds may be used to administer any election for Federal office in a State unless the State has in effect a law that prohibits an individual from the knowing collection and transmission of a ballot in an election for Federal office that was mailed to another person, other than an individual described as follows:

"(1) An election official while engaged in official duties as authorized by law.

"(2) An employee of the United States Postal Service or other commercial common carrier engaged in similar activities while engaged in duties authorized by law.

"(3) Any other individual who is allowed by law to collect and transmit United States mail, while engaged in official duties as authorized by law.

"(4) A family member, household member, or caregiver of the person to whom the ballot was mailed.

"(b) DEFINITIONS.—For purposes of this section, with respect to a person to whom the ballot was mailed:

"(1) The term 'caregiver' means an individual who provides medical or health care assistance to such person 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.

"(2) The term 'family member' means an individual who is related to such person by blood, marriage, adoption or legal guardianship.

"(3) The term 'household member' means an individual who resides at the same residence as such person.".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end the following new item:

"Sec. 908. Prohibition on Federal funds for election administration for States allowing collection and transmission of ballots by certain third parties.".

SEC. 136. CLARIFICATION WITH RESPECT TO FEDERAL ELECTION RECORD-KEEPING REQUIREMENT.

Section 301 of the Civil Rights Act of 1960 (52 U.S.C. 20701) is amended by inserting “ including envelopes used to deliver voted ballots by mail **[***New:***]** (but excluding envelopes used to deliver blank ballots or absentee ballot requests or used for any purpose other than delivering voted ballots),'' after ‘‘requisite to voting in such election,''.

SEC. 137. CLARIFICATION OF RULES WITH RESPECT TO HIRING OF ELECTION WORKERS.

(a) PREFERENCES FOR VETERANS AND INDIVIDUALS WITH DISABILITIES.—

(1) PREFERENCES.—In hiring election workers to administer an election in a State or local jurisdiction, the State or local jurisdiction may give preference to individuals who are veterans or individuals with a disability.

(2) INDIVIDUAL WITH A DISABILITY DEFINED.—In this subsection, an ‘‘individual with a disability'' means an individual with an impairment that substantially limits any major life activities.

(b) **[***New:***]** Preference and Waiver of Residency Requirement for Spouses and Dependents of Absent Military Voters.—

(1) PREFERENCE AND WAIVERS.—In hiring election workers to administer an election in a State or local jurisdiction, the State or local jurisdiction—

(A) may give preference to an individual who is a nonresident military spouse or dependent; and

(B) may not refuse to hire such an individual as an election worker solely on the grounds that the individual does not maintain a place of residence in the State or local jurisdiction.

(2) NONRESIDENT MILITARY SPOUSE OR DEPENDENT DEFINED.—In this subsection, a ‘‘nonresident military spouse or dependent’’ means an individual who is an absent uniformed services voter under section 107(1)(C) of the Uniformed and Overseas Citizen Absentee Voting Act (52 U.S.C. 20310(1)(C)).

SEC. 138. UNITED STATES POSTAL SERVICE COORDINATION WITH STATES TO ENSURE MAILING ADDRESSES.

(a) IN GENERAL.—Not later than 2 years after the date of the enactment of this Act, the Postmaster General shall, in coordination with the appropriate State executives of each State, carry out a program to identify and assign a mailing address to each home in each State that, as of the date of the enactment of this Act, does not have a mailing address assigned to such home, with a priority given to assigning mailing addresses to such homes located on Indian lands.

(b) DEFINITIONS.—In this section:

(1) INDIAN.—The term "Indian" has the meaning given the term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(2) INDIAN LANDS.—The term "Indian lands" includes—

(A) any Indian country of an Indian Tribe, as defined under section 1151 of title 18, United States Code;

(B) any land in Alaska owned, pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.), by an Indian Tribe that is a Native village (as defined in section 3 of that Act (43 U.S.C. 1602)) or by a Village Corporation that is associated with an Indian Tribe (as defined in section 3 of that Act (43 U.S.C. 1602));

(C) any land on which the seat of the Tribal Government is located; and

(D) any land that is part or all of a Tribal designated statistical area associated with an Indian Tribe, or is part or all of an Alaska Native village statistical area associated with an Indian Tribe, as defined by the Census Bureau for the purposes of the most recent decennial census.

(3) INDIAN TRIBE.—The term ''Indian Tribe'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(4) STATE.—The term ''State'' has the meaning given such term in section 901 of the Help America Vote Act of 2002 (52 U.S.C. 21141).

(5) TRIBAL GOVERNMENT.—The term ''Tribal Government'' means the recognized governing body of an Indian Tribe.

(c) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated $5,000,000 to carry out this section.

SEC. 139. STATE DEFINED.

Section 901 of the Help America Vote Act of 2002 (52 U.S.C. 21141) is amended by striking ''and the United States Virgin Islands'' and inserting ''the United

States Virgin Islands, and the Commonwealth of the Northern Mariana Islands''.

Subtitle D—District of Columbia Election Integrity and Voter Confidence

SEC. 141. SHORT TITLE.

This subtitle may be cited as the ''American Confidence in Elections: District of Columbia Election Integrity and Voter Confidence Act''.

SEC. 142. FINDINGS.

Congress finds the following:

(1) **[***to be provided***]**

SEC. 143. REQUIREMENTS FOR ELECTIONS IN DISTRICT OF COLUMBIA.

(a) Requirements Described.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21801 et seq.) is amended by adding at the end the following new subtitle:

"Subtitle C—Requirements for Elections in District of Columbia

"SEC. 321. STATEMENT OF CONGRESSIONAL AUTHORITY; FINDINGS.

''Congress finds that it has the authority to establish the terms and conditions for the administration of elections for public office in the District of Columbia—

"(1) under article I, section 8, clause 17 of the Constitution of the United States, which grants Congress the exclusive power to enact legislation with respect to the seat of the government of the United States; and

"(2) under other enumerated powers granted to Congress.

"SEC. 322. REQUIREMENTS FOR PHOTO IDENTIFICATION.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Voter Identification Act'.

"(b) REQUIRING PROVISION OF IDENTIFICATION TO RECEIVE A BALLOT OR VOTE.—

"(1) INDIVIDUALS VOTING IN PERSON.—A District of Columbia election official may not provide a ballot for a District of Columbia election to an individual who desires to vote in person unless the individual presents to the official an identification described in paragraph (3).

"(2) INDIVIDUALS VOTING OTHER THAN IN PERSON.—A District of Columbia election official may not provide a ballot for a District of Columbia election to an individual who desires to vote other than in person unless the individual submits with the application for the ballot a copy of an identification described in paragraph (3).

"(3) IDENTIFICATION DESCRIBED.—An identification described in this paragraph is, with respect to an individual, any of the following:

"(A) A current and valid motor vehicle license issued by the District of Columbia or any other current and valid photo identification of the individual which is issued by the District of Columbia or the identification number for such motor vehicle license or photo identification.

"(B) A current and valid United States passport, a current and valid military photo identification, or any other current and valid photo identification of the individual which is issued by the Federal government.

"(C) Any current and valid photo identification of the individual which is issued by a Tribal Government.

"(D) A student photo identification issued by a secondary school (as such term is defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801)) or an institution of higher education (as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001)).

"(E) The last 4 digits of the individual's social security number.

"(4) ENSURING PROOF OF RESIDENCE.—If an individual presents or submits an identification described in paragraph (3) which does not include the address of the individual's residence, the District of Columbia election official may not provide a ballot to the individual unless the individual presents or submits a document or other written information from a third party which—

"(A) provides the address of the individual's residence; and

"(B) such document or other written information is of sufficient validity such that the election official is reasonably certain as to the identity of the individual.

"(c) PROVISION OF IDENTIFICATION WITHOUT COST TO INDIGENT INDIVIDUALS.—If the District of Columbia charges an individual a fee for an identification described in subsection (b)(3) and the individual provides an attestation that the individual is unable to afford the fee, the District of Columbia shall provide the identification to the individual at no cost.

"(d) SPECIAL RULE WITH RESPECT TO SINCERELY HELD RELIGIOUS BELIEFS.—In the case of an individual who is unable to comply with the requirements of subsection (b) due to sincerely held religious beliefs, the District of Columbia shall provide such individual with an alternative identification that shall be deemed to meet the requirements of an identification described in subsection (b)(3).

"(e) DESIGNATION OF DISTRICT OF COLUMBIA AGENCY TO PROVIDE COPIES OF IDENTIFICATION.—The Mayor of the District of Columbia shall designate an agency of the District of Columbia government to provide an individual with a copy of an identification described in subsection (b)(3) at no cost to the individual for the purposes of meeting the requirement under subsection (b)(2).

"(f) INCLUSION OF PHOTOS IN POLL BOOKS.—

"(1) METHODS FOR OBTAINING PHOTOS.—

"(A) PROVISION OF PHOTOS BY OFFICES OF DISTRICT OF COLUMBIA GOVERNMENT.—If any office of the District of Columbia government has a photograph or digital image of the likeness of an individual who is eligible to vote in a District of Columbia election, the office, in consultation with the chief election official of the District of Columbia, shall provide access to the photograph or digital image to the chief election official of the District of Columbia.

"(B) TAKING OF PHOTOS AT POLLING PLACE.—If a photograph or digital image of an individual who votes in person at a polling place is not included in the poll book which contains the name of the individuals who are eligible to vote in the District of Columbia election and which is used by election officials to provide ballots to such eligible individuals, the appropriate election official shall take a photograph of the individual and provide access to the photograph to the chief election official of the District of Columbia.

"(C) COPIES OF PHOTOS PROVIDED BY INDIVIDUALS NOT VOTING IN PERSON.—The election official who receives a copy of an identification described in subsection (b)(3) which is submitted by an individual who desires to vote other than in person at a polling place shall provide access to the copy of the identification to the chief election official of the District of Columbia.

"(2) INCLUSION IN POLL BOOKS.—The chief election official of the District of Columbia shall ensure that a photograph, digital image, or copy of an identification for which access is provided under paragraph (1) is included in the poll book which contains the name of the individuals who are eligible to vote in the District of Columbia election and which is used by election officials to provide ballots to such eligible individuals.

"(3) PROTECTION OF PRIVACY OF VOTERS.—The appropriate election officials of the District of Columbia shall ensure that any photograph, digital image, or copy of an identification which is included in a poll book under this subsection is not used for any purpose other than the administration of District of Columbia elections and is not provided or otherwise made available to any other person except as may be necessary to carry out that purpose.

"(g) EXCEPTIONS.—This section does not apply with respect to any individual who is—

"(1) entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.);

"(2) provided the right to vote otherwise than in person under section 3(b)(2)(B)(ii) of the Voting Accessibility for the Elderly and Handicapped Act (52 U.S.C. 20102(b)(2)(B)(ii)); or

"(3) entitled to vote otherwise than in person under any other Federal law.

"(h) DEFINITIONS.—For the purposes of this section, the following definitions apply:

"(1) INDIAN TRIBE.—The term 'Indian Tribe' has the meaning given the term 'Indian tribe' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

"(2) TRIBAL GOVERNMENT.—The term 'Tribal Government' means the recognized governing body of an Indian Tribe.

"SEC. 323. REQUIREMENTS FOR VOTER REGISTRATION.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Voter List Maintenance Act'.

"(b) ANNUAL LIST MAINTENANCE.—

"(1) REQUIREMENTS.—

"(A) IN GENERAL.—The District of Columbia shall carry out annually a program to remove ineligible persons from the official list of persons registered to vote in the District of Columbia, as required by section 8 of the National Voter Registration Act of 1993 (52 U.S.C. 20507) and pursuant to the procedures described in subparagraph (B).

"(B) REMOVAL FROM VOTER ROLLS.—In the case of a registrant from the official list of eligible voters in District of Columbia elections who has failed to vote in a District of Columbia election during a period of two consecutive years, the District of Columbia shall send to such registrant a notice described in section 8(d)(2) of the National Voter Registration Act of 1993 (52 U.S.C. 20507(d)(2)) and shall remove the registrant from the official list of eligible voters in District of Columbia elections if—

"(i) the registrant fails to respond to such notice; and

"(ii) the registrant has not voted or appeared to vote in a District of Columbia election during the period beginning the date such notice is sent and ending the later of 4 years after the date such notice is sent or after two consecutive District of Columbia general elections have been held.

"(2) TIMING.—In the case of a year during which a regularly scheduled District of Columbia election is held, the District of Columbia shall carry out the program described in paragraph (1) not later than 90 days prior to the date of the election.

"(c) PROHIBITING SAME-DAY REGISTRATION.—The District of Columbia may not permit an individual to vote in a District of Columbia election unless, not later than 30 days prior to the date of the election, the individual is duly registered to vote in the election.

"SEC. 324. BAN ON COLLECTION AND TRANSMISSION OF BALLOTS BY CERTAIN THIRD PARTIES.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Election Fraud Prevention Act'.

"(b) IN GENERAL.—The District of Columbia may not permit an individual to knowingly collect and transmit a ballot in a District of Columbia election that was mailed to another person, other than an individual described as follows:

"(1) An election official while engaged in official duties as authorized by law.

"(2) An employee of the United States Postal Service or other commercial common carrier engaged in similar activities while engaged in duties authorized by law.

"(3) Any other individual who is allowed by law to collect and transmit United States mail, while engaged in official duties as authorized by law.

"(4) A family member, household member, or caregiver of the person to whom the ballot was mailed.

"(c) DEFINITIONS.—For purposes of this section, with respect to a person to whom the ballot was mailed:

"(1) The term 'caregiver' means an individual who provides medical or health care assistance to such person 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.

"(2) The term 'family member' means an individual who is related to such person by blood, marriage, adoption or legal guardianship.

"(3) The term 'household member' means an individual who resides at the same residence as such person.

"SEC. 325. TIMELY PROCESSING AND REPORTING OF RESULTS.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Timely Reporting of Election Results Act'.

"(b) TIME FOR PROCESSING BALLOTS AND REPORTING RESULTS.— The District of Columbia shall begin processing ballots received by mail in a District of Columbia election as soon as such ballots are received and shall ensure **[***New:***]** to the greatest extent practicable that the results of such District of Columbia election are reported to the public not later than 10:00 am on the date following the date of the election, but in no case shall such ballots be tabulated or such results be reported earlier than the closing of polls on the date of the election.

"(c) REQUIREMENT TO PUBLISH NUMBER OF VOTED BALLOTS ON ELECTION DAY.—The District of Columbia shall, as soon as practicable after the closing of polls on the date of a District of Columbia election, make available on a publicly accessible website the total number of voted ballots in the possession of election officials in the District of Columbia as of the time of the closing of polls on the date of such election, which shall include, as of such time—

"(1) the number of voted ballots delivered by mail;

"(2) the number of ballots requested for such election by individuals who are entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.); and

"(3) the number of voted ballots for such election received from individuals who are entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.), including from individuals who, under such Act, voted by absentee ballot without requesting such a ballot.

"(d) REQUIREMENTS TO ENSURE BIPARTISAN ELECTION ADMINISTRATION ACTIVITY.—With respect to a District of Columbia election, District of Columbia election officials shall ensure that all activities are carried out in a bipartisan manner, which shall include a requirement that, in the case of an election worker who enters a room which contains ballots, voting equipment, or non-voting equipment as any part of the election worker's duties to carry out such election, the election worker is accompanied by an individual registered to vote with respect to a different political party than such election worker, as determined pursuant to the voting registration records of the District of Columbia.

"SEC. 326. BAN ON NONCITIZEN VOTING.

''(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Citizen Voter Act'.

''(b) BAN ON NONCITIZEN VOTING.—No individual may vote in a District of Columbia election unless the individual is a citizen of the United States.

"SEC. 327. REQUIREMENTS WITH RESPECT TO PROVISIONAL BALLOTS.

''(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Provisional Ballot Reform Act'.

''(b) IN GENERAL.—Except as provided in subsection (c), the District of Columbia shall permit an individual to cast a provisional ballot pursuant to section 302 if—

''(1) the individual declares that such individual is a registered voter in the District of Columbia and is eligible to vote in a District of Columbia election but the name of the individual does not appear on the official list of eligible voters for the polling place or an election official asserts that the individual is not eligible to vote; or

''(2) the individual declares that such individual is a registered voter in the District of Columbia and is eligible to vote in a District of Columbia election but does not provide an identification required under section 322, except that the individual's provisional ballot shall not be counted in the election unless the individual provides such identification to the chief State election official of the District of Columbia not later than 5:00 pm on the second day which begins after the date of the election.

"(c) Requirements With Respect to Counting Provisional Ballots in Certain Cases.—If the name of an individual who is a registered voter in the District of Columbia and eligible to vote in a District of Columbia election appears on the official list of eligible voters for a polling place in the District of Columbia, such individual may cast a provisional ballot pursuant to section 302 for such election at a polling place other than the polling place with respect to which the name of the individual appears on the official list of eligible voters, except that the individual's provisional ballot shall not be counted in the election unless the individual demonstrates pursuant to the requirements under section 302 that the individual is a registered voter in the jurisdiction of the polling place at which the individual cast such ballot.

"SEC. 328. MANDATORY POST-ELECTION AUDITS.

"(a) Short Title.—This section may be cited as the 'American Confidence in Elections: District of Columbia Mandatory Post-Election Audits Act'.

"(b) REQUIREMENT FOR POST-ELECTION AUDITS.—Not later than 30 days after each District of Columbia election, the District of Columbia shall conduct and publish an audit of the effectiveness and accuracy of the voting systems used to carry out the election and the performance of the election officials who carried out the election, but in no case shall such audit be completed later than 2 business days before the deadline to file an election contest under the laws of the District of Columbia.

"SEC. 329. PUBLIC OBSERVATION OF ELECTION PROCEDURES.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Public Observation of Election Procedures Act'.

"(b) DESIGNATED REPRESENTATIVES OF CANDIDATES, POLITICAL PARTIES, AND COMMITTEES AFFILIATED WITH BALLOT INITIATIVES.—

"(1) AUTHORITY TO OBSERVE PROCEDURES.—An individual who is not a District of Columbia election official may observe election procedures carried out in a District of Columbia election, as described in paragraph (2), if the individual is designated to observe such procedures by a candidate in the election, a political party, or a committee affiliated with a ballot initiative or referendum in the election.

"(2) AUTHORITY AND PROCEDURES DESCRIBED.—The authority of an individual to observe election procedures pursuant to this subsection is as follows:

"(A) The individual may serve as a poll watcher to observe the casting and tabulation of ballots at a polling place on the date of the election or on any day prior to the date of the election on which ballots are cast at early voting sites, and may challenge the casting or tabulation of any such ballot.

"(B) The individual may serve as a poll watcher to observe the canvassing and processing of absentee or other mail-in ballots, including the procedures for verification of signed certificates of transmission under section 330(c)(2).

"(C) The individual may observe the recount of the results of the election at any location at which the recount is held, and may challenge the tabulation of any ballot tabulated pursuant to the recount.

"(3) PROVISION OF CREDENTIALS.—The chief State election official of the District of Columbia shall provide each individual who is authorized to observe election procedures under paragraph (1) with appropriate credentials to enable the individual to observe such procedures.

"(4) EXCEPTION FOR CANDIDATES AND LAW ENFORCEMENT OFFICERS.—An individual may not serve as a poll watcher under subparagraph (A) or (B) of paragraph (2), and the chief State election official of the District of Columbia may not provide the individual with credentials to enable the individual to serve as a poll watcher under such subparagraph, if the individual is a candidate in the election or a law enforcement officer.

"(c) OTHER INDIVIDUALS.—

"(1) PETITION FOR OBSERVER CREDENTIALS.—In addition to the individuals described in subsection (b), any individual, including an individual representing or affiliated with a domestic or international organization, may petition the chief State election official of the District of Columbia to provide the individual with credentials to observe election procedures carried out in a District of Columbia election, as described in subsection (b).

"(2) AUTHORITY DESCRIBED.—If the chief State election official provides an individual with credentials under paragraph (1), the individual shall have the same authority to observe election procedures carried out in the election as an individual described in subsection (b), except that the individual may not challenge the casting, tabulation, canvassing, or processing of any ballot in the election.

"(3) EXCEPTION FOR CANDIDATES AND LAW ENFORCEMENT OFFICERS.—The chief State election official of the District of Columbia may not provide an individual who is a candidate in the election or a law enforcement officer with credentials to serve as a poll watcher, as described in subparagraph (A) or (B) of subsection (b)(2).

"(d) AUTHORITY OF MEMBERS OF PUBLIC TO OBSERVE TESTING OF EQUIPMENT.—In addition to the authority of individuals to observe procedures under subsections (b) and (c), any member of the public may observe the testing of election equipment by election officials prior to the date of the election.

"(e) PROHIBITING LIMITS ON ABILITY TO VIEW PROCEDURES.—An election official may not obstruct the ability of an individual who is authorized to observe an election procedure under this section to view the procedure as it is being carried out.

"(f) PROHIBITION AGAINST CERTAIN RESTRICTIONS.—An election official may not require that an individual who observes election procedures under this section stays more than 3 feet away from the procedure as it is being carried out.

"SEC. 330. REQUIREMENTS FOR VOTING BY MAIL-IN BALLOT.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Mail Balloting Reform Act'.

"(b) PROHIBITING TRANSMISSION OF UNSOLICITED BALLOTS.—The District of Columbia may not transmit an absentee or other mail-in ballot for a District of Columbia election to any individual who does not request the District of Columbia to transmit the ballot.

"(c) SIGNATURE VERIFICATION.—

"(1) INCLUSION OF CERTIFICATE WITH BALLOT.—The District of Columbia shall include with each absentee or other mail-in ballot transmitted for a District of Columbia election a certificate of transmission which may be signed by the individual for whom the ballot is transmitted.

"(2) REQUIRING VERIFICATION FOR BALLOT TO BE COUNTED.—Except as provided in subsection (d), the District of Columbia may not accept an absentee or other mail-in ballot for a District of Columbia election unless—

"(A) the individual for whom the ballot was transmitted—

"(i) signs and dates the certificate of transmission included with the ballot under paragraph (1); and

"(ii) includes the signed certification with the ballot and the date on such certification is accurate and in no case later than the date of the election; and

"(B) the individual's signature on the ballot matches the signature of the individual on the official list of registered voters in the District of Columbia or other official record or document used by the District of Columbia to verify the signatures of voters.

"(d) NOTICE AND OPPORTUNITY TO CURE.—

"(1) NOTICE AND OPPORTUNITY TO CURE DISCREPANCY IN SIGNATURES.—If an individual submits an absentee or other mail-in ballot for a District of Columbia election and the appropriate District of Columbia election official determines that a discrepancy exists between the signature on such ballot and the signature of such individual on the official list of registered voters in the District of Columbia or other official record or document used by the District of Columbia to verify the signatures of voters, such election official, prior to making a final determination as to the validity of such ballot, shall—

"(A) make a good faith effort to immediately notify the individual by mail, telephone, or (if available) text message and electronic mail that—

"(i) a discrepancy exists between the signature on such ballot and the signature of the individual on the official list of registered voters in the District of Columbia or other official record or document used by the District of Columbia to verify the signatures of voters; and

"(ii) if such discrepancy is not cured prior to the expiration of the 48-hour period which begins on the date the official notifies the individual of the discrepancy, such ballot will not be counted; and

"(B) cure such discrepancy and count the ballot if, prior to the expiration of the 48-hour period described in subparagraph (A)(ii), the individual provides the official with information to cure such discrepancy, either in person, by telephone, or by electronic methods.

"(2) NOTICE AND OPPORTUNITY TO CURE MISSING SIGNATURE OR OTHER DEFECT.—If an individual submits an absentee or other mail-in ballot for a District of Columbia election without a signature on the ballot or the certificate of transmission included with the ballot under subsection (c)(1) or submits an absentee ballot with another defect which, if left uncured, would cause the ballot to not be counted, the appropriate District of Columbia election official, prior to making a final determination as to the validity of the ballot, shall—

"(A) make a good faith effort to immediately notify the individual by mail, telephone, or (if available) text message and electronic mail that—

"(i) the ballot or certificate of transmission did not include a signature or has some other defect; and

"(ii) if the individual does not provide the missing signature or cure the other defect prior to the expiration of the 48-hour period which begins on the date the official notifies the individual that the ballot or certificate of transmission did not include a signature or has some other defect, such ballot will not be counted; and

"(B) count the ballot if, prior to the expiration of the 48-hour period described in subparagraph (A)(ii), the individual provides the official with the missing signature on a form proscribed by the District of Columbia or cures the other defect.

This paragraph does not apply with respect to a defect consisting of the failure of a ballot to meet the applicable deadline for the acceptance of the ballot, as described in subsection (e).

"(e) DEADLINE FOR ACCEPTANCE.—

"(1) DEADLINE.—Except as provided in paragraph (2), the District of Columbia may not accept an absentee or other mail-in ballot for a District of Columbia election which is received by the appropriate election official following the close of polls on Election Day.

"(2) EXCEPTION FOR ABSENT MILITARY AND OVERSEAS VOTERS.—Paragraph (1) does not apply to a ballot cast by an individual who is entitled to vote by absentee ballot under the Uniformed and

Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.).

"(3) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed as prohibiting the District of Columbia from accepting an absentee or other mail-in ballot for a District of Columbia election that is delivered in person by the voter to an election official at an appropriate polling place or the District of Columbia Board of Elections if such ballot is received by the election official by the deadline described in paragraph (1).

"SEC. 331. REQUIREMENTS WITH RESPECT TO USE OF DROP BOXES.

"(a) SHORT TITLE.—This section may be cited as the 'American Confidence in Elections: District of Columbia Ballot Security Act'.

"(b) REQUIREMENTS.—With respect to a District of Columbia election, the District of Columbia may not use a drop box to accept a voted absentee or other mail-in ballot for any such election unless—

"(1) any such drop box is located inside a District of Columbia government building or facility;

"(2) the District of Columbia provides for the security of any such drop box through 24-hour remote or electronic surveillance; and

"(3) the District of Columbia Board of Elections collects any ballot deposited in any such drop box each day after 5:00 p.m. (local time) during the period of the election.

"SEC. 332. SPECIAL RULE WITH RESPECT TO APPLICATION OF REQUIREMENTS TO FEDERAL ELECTIONS.

"With respect to an election for Federal office in the District of Columbia, to the extent that there is any inconsistency with the requirements of this subtitle and the requirements of subtitle A, the requirements of this subtitle shall apply.

"SEC. 333. DISTRICT OF COLUMBIA ELECTION DEFINED.

"In this subtitle, the term 'District of Columbia election' means any election for public office in the District of Columbia, including an election for Federal office, and any ballot initiative or referendum.".

(b) CONFORMING AMENDMENT RELATING TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking the period at the end and inserting the following: ", and the requirements of subtitle C with respect to the District of Columbia.".

(c) CLERICAL AMENDMENT.—The table of contents of such Act is amended by adding at the end of the items relating to title III the following:

"Subtitle C—Requirements for Elections in District of Columbia

SEC. 144. EFFECTIVE DATE.

The amendments made by this subtitle shall apply with respect to District of Columbia elections held on or after January 1, 2024. For purposes of this section, the term ''District of Columbia election'' has the meaning given such term in section 333 of the Help America Vote Act of 2002, as added by section 143(a).

Subtitle E—Administration of the Election Assistance Commission

SEC. 151. SHORT TITLE.

This subtitle may be cited as the ''Positioning the Election Assistance Commission for the Future Act of 2022''.

SEC. 152. FINDINGS RELATING TO THE ADMINISTRATION OF THE ELECTION ASSISTANCE COMMISSION.

Congress finds the following:

(1) The Election Assistance Commission best serves the American people when operating within

its core statutory functions, including serving as a clearinghouse for information on election administration, providing grants, and testing and certifying election equipment.

(2) The American people are best served when Federal agency election assistance is offered by a single agency with expertise in this space. The Election Assistance Commission, composed of four election experts from different political parties, is best situated among the Federal government agencies to offer assistance services to citizens and to guide other Federal agencies that have responsibilities in the elections space. The Commission is also best suited to determine the timing of the issuance of any advisories and to disburse all appropriated election grant funding.

(3) To this end, Congress finds that the Election Assistance Commission should be viewed as the lead Federal government agency on all election administration matters, and other Federal agencies operating in this space should look to the Commission for guidance, direction, and support on election administration-related issues.

SEC. 153. REQUIREMENTS WITH RESPECT TO STAFF AND FUNDING OF THE ELECTION ASSISTANCE COMMISSION.

(a) STAFF.—Section 204(a)(5) of the Help America Vote Act of 2002 (52 U.S.C. 20924(a)(5)) is amended by striking ‘‘of such additional personnel’’ and inserting ‘‘of not more than 55 full-time equivalent employees to carry out the duties and responsibilities under this Act and the additional duties and responsibilities required under the American Confidence in Elections Act’’.

(b) FUNDING.—Section 210 of the Help America Vote Act of 2002 (52 U.S.C. 20930) is amended—

(1) by striking ‘‘for each of the fiscal years 2003 through 2005’’ and inserting ‘‘for each of the fiscal years 2023 through 2025’’; and

(2) by striking ‘‘(but not to exceed $10,000,000 for each such year)’’ and inserting ‘‘(but not to exceed $25,000,000 for each such year)’’.

(c) PROHIBITION ON CERTAIN USE OF FUNDS.—

(1) PROHIBITION.—None of the funds authorized to be appropriated or otherwise made available under subsection (b) may be obligated or expended for the operation of an advisory committee established by the Election Assistance Commission pursuant to and in accordance with the provisions of the Federal Advisory Committee Act (5 U.S.C. App. 2),

except with respect to the operation of the Local Leadership Council.

(2) NO EFFECT ON ENTITIES ESTABLISHED BY HELP AMERICA VOTE ACT OF 2002.—Paragraph (1) does not apply with respect to the operation of any entity established by the Help America Vote Act of 2002, including the Election Assistance Commission Standards Board, the Election Assistance Commission Board of Advisors, and the Technical Guidelines Development Committee.

(d) REQUIREMENTS WITH RESPECT TO COMPENSATION OF MEMBERS OF THE COMMISSION.—Section 203(d) of the Help America Vote Act of 2002 (52 U.S.C. 20923(d)) is amended—

(1) in paragraph (1), by striking ''at the annual rate of basic pay prescribed for level IV of the Executive Schedule under section 5315 of title 5, United States Code'' and inserting ''at an annual rate of basic pay equal to the amount of $186,300, as adjusted under section 5318 of title 5, United States Code, in the same manner as the annual rate of pay for positions at each level of the Executive Schedule'';

(2) in paragraph (2), by striking ‘‘No member appointed’’ and inserting ‘‘Except as provided in paragraph (3), no member appointed’’; and

(3) by adding at the end the following new paragraph:

‘‘(3) SUPPLEMENTAL EMPLOYMENT AND COMPENSATION.—An individual serving a term of service on the Commission shall be permitted to hold a position at an institution of higher education (as such term is defined in section 101 of the Higher Education Act of 1965 (20 U.S.C. 1001) if—

‘‘(A) the ❲*New:*❳ General Counsel of the Election Assistance Commission determines that such position does not create a conflict of interest with the individual’s position as a sitting member of the Commission and grants the individual approval to hold the position; and

‘‘(B) the annual rate of compensation received by the individual from such institution is not greater than the amount equal to 49.9% of the annual rate of basic pay paid to the individual under paragraph (1).’’.

(e) OFFICE OF INSPECTOR GENERAL.—Section 204 of the Help America Vote Act of 2002 (52 U.S.C. 20924) is amended by adding at the end the following new subsection:

"(f) OFFICE OF INSPECTOR GENERAL.—The Inspector General of the Election Assistance Commission may appoint not more than 7 full-time equivalent employees to assist the Inspector General to carry out the duties and responsibilities under [*Revised to reflect enactment of IG Act as part of title 5, United States Code:*] section 404 of title 5, United States Code, of whom 2 shall have primarily administrative duties and responsibilities.".

(f) EFFECTIVE DATE.—This section and the amendments made by this section shall take effect on October 1, 2022.

SEC. 154. GENERAL REQUIREMENTS FOR PAYMENTS MADE BY ELECTION ASSISTANCE COMMISSION.

(a) EXCLUSIVE AUTHORITY OF ELECTION ASSISTANCE COMMISSION TO MAKE ELECTION ADMINISTRATION PAYMENTS TO STATES.—No entity of the Federal Government other than the Election Assistance Commission may make any payment to a State for purposes of administering elections for Federal office, including obtaining election and voting equipment and infrastructure, enhancing election and voting technology, and making election and voting security improvements, including with respect to cybersecurity and infrastructure.

(b) ⟦*New:*⟧ Prohibiting Use of Payments for Get-out-the-vote-activity.—Subtitle D of title II of the Help America Vote Act of 2002 (52 U.S.C. 21001 et seq.) is amended by adding at the end the following new part:

"PART 7—GENERAL REQUIREMENTS FOR PAYMENTS

"SEC. 297. PROHIBITING USE OF PAYMENTS FOR GET-OUT-THE-VOTE-ACTIVITY.

''(a) Prohibition.—No payment made to a State or unit of local government by the Commission ⟦*Review: Do you want or need to include this to clarify the application of this restriction to funds that don't consist of requirements payments under HAVA?* under this Act or any other Act⟧ may be used for get-out-the-vote activity.

''(b) Definition.—In this section, the term 'get-out-the-vote activity' means, with respect to a payment made to a State or unit of local government, any activity which, at the time the payment is made, is treated as get-out-the-vote-activity under the Federal Election Campaign Act of 1971 and the regulations promulgated by the Federal Election Commission to carry out such Act. ⟦*Q: Do you want or need to carve out an exception for activity described in 11 CFR 100.24(a)(3)(i)(B)(1) (informing voters about times when polling places are open) or (B)(2) (informing voters about the location of particular polling places)?*⟧''.

(c) ⟦*New:*⟧ Requiring Disclaimer in Communications.—Part 7 of subtitle D of title II of such Act, as added by subsection (b), is amended by adding at the end the following new section:

"SEC. 297A. REQUIRING COMMUNICATIONS FUNDED BY PAYMENTS TO INCLUDE DISCLAIMER.

"(a) Requirement.—⟦*Note: This is drafted on the assumption that the requirement applies only to communications developed or disseminated by a recipient of EAC funds and not to the EAC's own public communications. Is that a correct assumption?*⟧ If a State or unit of local government disseminates a public communication which was developed or disseminated in whole or in part with a payment made to the State or local government by the Commission ⟦*See note above:* under this Act or any other Act⟧, the State or unit of local government shall ensure that the communication includes, in a clear and conspicuous manner, the following statement: 'Paid for using Federal taxpayer funds pursuant to the Help America Vote Act'.

"(b) Clear and Conspicuous Manner Described.—⟦*Based on H.R. 3044, 118th:*⟧ A statement required under subsection (a) shall be considered to be in a clear and conspicuous manner if the statement meets the following requirements:

"(1) TEXT OR GRAPHIC COMMUNICATIONS.—In the case of a text or graphic communication, the statement—

"(A) appears in letters at least as large as the majority of the text in the communication

"(B) is contained in a printed box set apart from the other contents of the communication; and

"(C) is printed with a reasonable degree of color contrast between the background and the printed statement.

"(2) AUDIO COMMUNICATIONS.—In the case of an audio communication, the statement is spoken in a clearly audible and intelligible manner at the beginning or end of the communication and lasts at least 3 seconds.

"(3) VIDEO COMMUNICATIONS.—In the case of a video communication which also includes audio, the statement—

"(A) is included at either the beginning or the end of the communication; and

"(B) is made both in—

"(i) a written format that meets the requirements of subparagraph (A) and appears for at least 4 seconds; and ''(ii) an audible format that meets the requirements of subparagraph (B).

''(4) OTHER COMMUNICATIONS.—In the case of any other type of communication, the statement is at least as clear and conspicuous as the statement specified in paragraph (1), (2), or (3).

''(c) PUBLIC COMMUNICATION.—[*Based on section 301(20) of the FECA:*] In this section, the term 'public communication' means a communication [*Review:* relating to the administration of an election for Federal office] by means of any broadcast, cable, or satellite communication, newspaper, magazine, outdoor advertising facility, mass mailing, or telephone bank to the general public, or any other form of general public advertising.''.

(d) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting at the end of the items relating to subtitle D of title II the following:

''PART 7—GENERAL REQUIREMENTS FOR PAYMENTS

''Sec. 297. Prohibiting use of payments for get-out-the-vote-activity.
''Sec. 297A. Requiring communications funded by payments to include disclaimer.''.

(e) EFFECTIVE DATE.—This section and the amendments made by this section shall apply with respect to payments made on or after the date of the enactment of this Act.

SEC. 155. EXECUTIVE BOARD OF THE STANDARDS BOARD AUTHORITY TO ENTER INTO CONTRACTS.

Section 213(c) of the Help America Vote Act of 2002 (52 U.S.C. 20943(c)) is amended by adding at the end the following new paragraph:

"(5) Authority to enter into contracts.—The Executive Board of the Standards Board may, using amounts already made available to the Commission, enter into contracts to employ and retain no more than 2 individuals to enable the Standards Board to discharge its duties with respect to the examination and release of voluntary considerations with respect to the administration of elections for Federal offices by the States under section 247, except that—

"(A) no more than 1 individual from the same political party may be employed under such contracts at the same time;

"(B) the authority to enter into such contracts shall end on the earlier of the date of the release of the considerations or December 31, 2023; and

"(C) no additional funds may be appropriated to the Commission for the purposes of carrying out this paragraph.".

SEC. 156. ELECTION ASSISTANCE COMMISSION PRIMARY ROLE IN ELECTION ADMINISTRATION.

Except as provided in any other provision of law, the Election Assistance Commission shall, with respect to any other entity of the Federal Government, have primary jurisdiction to address issues with respect to the administration of elections for Federal office.

Subtitle F—Prohibition on Involvement in Elections by Foreign Nationals

SEC. 161. PROHIBITION ON CONTRIBUTIONS AND DONATIONS BY FOREIGN NATIONALS IN CONNECTION WITH BALLOT INITIATIVES AND REFERENDA.

(a) SHORT TITLE.—This section may be cited as the "Keeping Foreign Money out of Ballot Measures Act of 2022".

(b) IN GENERAL.—Chapter 29 of title 18, United States Code, is amended by adding at the end the following new section:

"§ 612. Foreign nationals making certain political contributions

"(a) PROHIBITION.—It shall be unlawful for a foreign national, directly or indirectly, to make a contribution as such term is defined in section 301(8)(A) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(8)(A)) or donation of money or other thing of value, or to make an express or implied promise to make a contribution or donation, in connection with a State or local ballot initiative or referendum.

"(b) PENALTY.—Any person who violates subsection (a) shall be fined not more than the greater of $10,000 or 300 percent of the amount of the contribution or value of the donation of money or other thing of value made by the person, imprisoned for not more than 1 year, or both.

"(c) FOREIGN NATIONAL DEFINED.—In this section, the term 'foreign national' has the meaning given such term in section 319(b) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30121(b)).".

(c) CLERICAL AMENDMENT.—The table of sections for chapter 29 of title 18, United States Code, is amended by adding at the end the following new item:

"612. Foreign nationals making certain political contributions.".

(d) EFFECTIVE DATE.—The amendment made by this section shall apply with respect to contributions and donations made on or after the date of the enactment of this Act.

Subtitle G—Constitutional Experts Panel With Respect to Presidential Elections

SEC. 171. SHORT TITLE.

This subtitle may be cited as the ''Solving an Overlooked Loophole in Votes for Executives (SOLVE) Act''.

SEC. 172. ESTABLISHMENT OF PANEL OF CONSTITUTIONAL EXPERTS.

(a) ESTABLISHMENT.—There is established the ''Twentieth Amendment Section Four Panel'' (in this section referred to as the ''Panel'').

(b) MEMBERSHIP.—

(1) IN GENERAL.—The Panel shall be composed of 6 constitutional experts, of whom—

(A) 1 shall be appointed by the majority leader of the Senate;

(B) 1 shall be appointed by the minority leader of the Senate;

(C) 1 shall be appointed jointly by the majority and minority leader of the Senate;

(D) 1 shall be appointed by the Speaker of the House of Representatives;

(E) 1 shall be appointed by minority leader of the House of Representatives; and

(F) 1 shall be appointed jointly by the Speaker of the House of Representatives and the minority leader of the House of Representatives.

(2) DATE.—The appointments of the members of the Panel shall be made not later than 180 days after the date of enactment of this Act.

(3) VACANCY.—Any vacancy occurring in the membership of the Panel shall be filled in the same manner in which the original appointment was made.

(4) CHAIRPERSON AND VICE CHAIRPERSON.—The Panel shall select a Chairperson and Vice Chairperson from among the members of the Panel.

(c) PURPOSE.—The purpose of the Panel shall be to recommend to Congress model legislation, which shall provide for an appropriate process, pursuant to section 4 of the Twentieth Amendment to the United States Constitution, to resolve any vacancy created by the death of a candidate in a contingent presidential or vice-presidential election.

(d) REPORTS.—

(1) INITIAL REPORT.—Not later than 1 year after the date on which all of the appointments have been made under subsection (b)(2), the Panel shall

submit to Congress an interim report containing the Panel's findings, conclusions, and recommendations.

(2) FINAL REPORT.—Not later than 6 months after the submission of the interim report under paragraph (1), the Panel shall submit to Congress a final report containing the Panel's findings, conclusions, and recommendations.

(e) MEETINGS; INFORMATION.—

(1) IN GENERAL.—Meetings of the Panel shall be held at the Law Library of Congress.

(2) INFORMATION.—The Panel may secure from the Law Library of Congress such information as the Panel considers necessary to carry out the provisions of this section.

(f) FUNDS.—

(1) COMPENSATION OF MEMBERS.—Members of the Panel shall receive no compensation.

(2) OTHER FUNDING.—No amounts shall be appropriated for the purposes of this section, except for any amounts strictly necessary for the Law Library of Congress to execute its responsibilities under subsection (e).

(g) TERMINATION.—

(1) IN GENERAL.—The panel established under subsection (a) shall terminate 90 days after the date

on which the panel submits the final report required under subsection (d)(2).

(2) RECORDS.—Upon termination of the panel, all of its records shall become the records of the Secretary of the Senate and the Clerk of the House of Representatives.

TITLE II—MILITARY VOTING ADMINISTRATION

SEC. 200. SHORT TITLE.

This title may be cited as the ‘‘American Confidence in Elections: Protecting American Servicemembers' and Dependents' Right to Vote Act''.

Subtitle A—Findings Relating to Military Voting

SEC. 201. FINDINGS RELATING TO MILITARY VOTING.

Congress finds the following:

(1) Participation in the voting process by Americans who serve in the Armed Forces is vital to the future of the Republic; however, due to the realities of service around the globe and despite many best efforts, the nation has not always lived up to its commitment to servicemembers that their vote be counted.

(2) The Military and Overseas Empowerment (MOVE) Act made great progress in solving prob-

lems with voting that many servicemembers faced. Yet, for many, it is still difficult to exercise the franchise, with many ballots not reaching State elections officials until after the deadline, negating their voice. After 13 years, Congress must address the remaining issues.

(3) Congress finds that it is a moral imperative of national importance that every eligible American servicemember has the opportunity to cast a ballot in each election and, not only that such ballot be received in time to be counted, but that it actually be counted according to law.

Subtitle B—GAO Analysis on Military Voting Access

SEC. 211. GAO ANALYSIS AND REPORT ON EFFECTIVENESS OF FEDERAL GOVERNMENT IN MEETING OBLIGATIONS TO PROMOTE VOTING ACCESS FOR ABSENT UNIFORMED SERVICES VOTERS.

(a) ANALYSIS.—The Comptroller General of the United States shall conduct an analysis of the effectiveness of the Federal government in carrying out its responsibilities under the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20301 et seq.) to promote access to voting for absent uniformed services voters.

(b) ISSUED ANALYZED.—In conducting the analysis under this section, the Comptroller General shall cover the following issues:

(1) The transmission of ballots to absent uniformed services voters.

(2) The methods of transmission of voted ballots from absent uniformed services voters, including the efficacy and security of such methods.

(3) The treatment by election officials of voted ballots transmitted by absent uniformed services voters, including the rate at which such ballots are counted in elections and the rate at which such ballots are rejected in elections and the reasons therefore.

(4) The effectiveness of the assistance provided to absent uniformed services voters by Voting Assistance Officers of the Federal Voting Assistance Program of the Department of Defense.

(5) The extent of the coordination between Voting Assistance Officers and State and local election officials.

(6) Such other issues relating to the ability of absent uniformed services voters to register to vote, vote, and have their ballots counted in elections for Federal office.

(c) METHOD OF ANALYSIS.—The Comptroller General shall base the analysis conducted under subsection (a) on existing information available government and other public sources, as well as information the Comptroller General shall acquire through the Comptroller General's own investigations, interviews, and analysis.

(d) REPORT.—Not later than December 31, 2023, the Comptroller General shall submit to the chair and ranking minority member of the Committee on House Administration of the House of Representatives and the chair and ranking minority member of the Committee on Rules and Administration of the Senate a report that contains the results of the analysis conducted under subsection (a).

(e) DEFINITION.—In this section, the term ''absent uniformed services voter'' has the meaning given such term in section 107(1) of the Uniformed and Overseas Citizens Absentee Voting Act (52 U.S.C. 20310(1)).

SEC. 212. STUDIES ON IMPROVING ACCESS TO VOTER REGISTRATION INFORMATION AND ASSISTANCE FOR MEMBERS OF THE ARMED FORCES.

(a) STUDIES REQUIRED.—

(1) IN GENERAL.—The Secretary of each military department shall conduct a study on means for improving access to voter registration information

and assistance for members of the military department and their family members.

(2) SURVEYS REQUIRED.—In conducting a study required by paragraph (1), the Secretary of each military department shall conduct a survey of members of the military department to assess—

(A) the awareness of those members of the requirement under section 1566a of title 10, United States Code, that the department to provide voter registration information and assistance to members; and

(B) whether those members received such information and assistance at the times required by subsection (c) of that section.

(b) REPORTS REQUIRED.—

(1) IN GENERAL.—Not later than September 30, 2025, the Secretary of each military department shall submit to Congress a report on the results of the study conducted by the Secretary under subsection (a)(1).

(2) ELEMENTS.—The report submitted by the Secretary of a military department under paragraph (1) shall include the following:

(A) The results of the survey conducted by the Secretary under subsection (a)(2).

(B) An estimate of the costs and requirements to fully meet the needs of members of the military department for access to voter registration information and assistance.

(C) A description and assessment of actions to be undertaken to increase access to voter registration information and assistance of members of the military department and their family members.

TITLE III—PROTECTION OF POLITICAL SPEECH AND CAMPAIGN FINANCE REFORM

Subtitle A—Protecting Political Speech

SEC. 301. FINDINGS.

Congress finds the following:

(1) The structure of the Constitution and its amendments represents the radical idea that any sovereign power exercised by the federal government flows either directly from the people or through the States they established to govern themselves. In the words of the Ninth and Tenth Amendments, ''[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.'' ''The powers not delegated

to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.''

(2) Among the many freedoms it protects, the First Amendment prevents Congress from making any law abridging the freedom of speech, the right of the people peaceably to assemble, or the right of the people to petition the Government for the redress of grievances.

(3) Any proposed federal action concerning freedom of speech, protest, or petition must start with an analysis of the First Amendment. Congress must ask whether the proposed action would abridge these freedoms, and any uncertainty must be determined in favor of fewer restrictions on speech.

(4) In particular, political speech, uttered in the furtherance of self-government, must raise an even higher bar to congressional abridgement. The mechanisms and media used to offer political speech must realize the same protections.

(5) As the Supreme Court has recognized, the Constitution grants Congress only a very narrow interest in the regulation of political speech, the prevention of corruption or the appearance of corruption.

(6) In order to uphold and effectuate the Constitution, any federal statute that goes beyond this interest must be repealed, and Congress must exercise its Article 1 authorities to do so.

SEC. 302. REPEAL OF LIMITS ON COORDINATED POLITICAL PARTY EXPENDITURES.

(a) REPEAL OF LIMITS.—Section 315(d) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30116(d)) is amended—

(1) in paragraph (1)—

(A) by striking ‘‘may make expenditures’’ and inserting ‘‘may make expenditures, including coordinated expenditures,’’, and

(B) by striking ‘‘Federal office, subject to the limitations contained in paragraphs (2), (3), and (4) of this subsection’’ and inserting ‘‘Federal office in any amount’’; and

(2) by striking paragraphs (2), (3), (4), and (5).

(b) CLARIFYING TREATMENT OF CERTAIN PARTY COMMUNICATIONS AS COORDINATED EXPENDITURES.—Section 315(d) of such Act (52 U.S.C. 30116(d)), as amended by subsection (a), is amended by adding at the end the following new paragraph:

"(2) For purposes of this subsection, if a public communication paid for by a committee of a political party or its agent refers to a clearly identified House or Senate candidate and is publicly distributed or otherwise publicly disseminated in the clearly identified candidate's jurisdiction, the communication shall be treated as a coordinated expenditure in connection with the campaign of a candidate for purposes of this subsection.".

(c) CONFORMING AMENDMENT RELATING TO INDEXING.—Section 315(c) of such Act (52 U.S.C. 30116(c)) is amended—

(1) in paragraph (1)(B)(i), by striking "(d),"; and

(2) in paragraph (2)(B)(i), by striking "subsections (b) and (d)" and inserting "subsection (b)".

(d) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 303. REPEAL OF LIMIT ON AGGREGATE CONTRIBUTIONS BY INDIVIDUALS.

(a) FINDINGS.—Congress finds that the Supreme Court of the United States in *McCutcheon v. FEC*, 572 U.S. 185 (2014) determined the biennial aggregate limits under section 315(a)(3) of the Federal Election Campaign

Act of 1971 (52 U.S.C. 30116(a)(3)) to be unconstitutional.

(b) REPEAL.—Section 315(a) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30116(a)) is amended by striking paragraph (3).

(c) CONFORMING AMENDMENTS.—Section 315(c) of such Act (52 U.S.C. 30116(c)) is amended by striking "(a)(3)," each place it appears in paragraph (1)(B)(i), (1)(C), and (2)(B)(ii).

SEC. 304. EQUALIZATION OF CONTRIBUTION LIMITS TO STATE AND NATIONAL POLITICAL PARTY COMMITTEES.

(a) IN GENERAL.—Section 315(a)(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30116(a)(1)) is amended—

(1) in subparagraph (B), by striking "a national political party" and inserting "a national or State political party";

(2) by adding "or" at the end of subparagraph (B);

(3) in subparagraph (C), by striking "; or" and inserting a period; and

(4) by striking subparagraph (D).

(b) CONTRIBUTIONS BY MULTICANDIDATE POLITICAL COMMITTEES.—

(1) IN GENERAL.—Section 315(a)(2)(B) of such Act (52 U.S.C. 30116(a)(2)(B)) is amended by striking ''a national political party'' and inserting ''a national or State political party''.

(2) PRICE INDEX ADJUSTMENT.—Section 315(c) of such Act (52 U.S.C. 30116(c)) is amended—

(A) in paragraph (1), by adding at the end the following new subparagraph:

''(D) In any calendar year after 2022—

''(i) a threshold established by subsection (a)(2) shall be increased by the percent difference determined under subparagraph (A);

''(ii) each amount so increased shall remain in effect for the calendar year; and

''(iii) if any amount after adjustment under clause (i) is not a multiple of $100, such amount shall be rounded to the nearest multiple of $100.''; and

(B) in paragraph (2)(B)—

(i) in clause (i), by striking ''and'' at the end;

(ii) in clause (ii), by striking the period at the end and inserting ''; and''; and

(iii) by adding at the end the following new clause:

''(iii) for purposes of subsection (a)(2), calendar year 2022.''.

(c) ACCEPTANCE OF ADDITIONAL AMOUNTS FOR CERTAIN ACCOUNTS.—

(1) PERMITTING ACCEPTANCE OF ADDITIONAL AMOUNTS IN SAME MANNER AS NATIONAL PARTIES.—Section 315(a) of such Act (52 U.S.C. 30116(a)) is amended—

(A) in paragraph (1)(B), by striking ''paragraph (9)'' and inserting ''paragraph (9) or paragraph (10)''; and

(B) in paragraph (2)(B), by striking ''paragraph (9)'' and inserting ''paragraph (9) or paragraph (10)''.

(2) ACCOUNTS.—Section 315(a)(9) of such Act (52 U.S.C. 30116(a)(9)) is amended by striking ''national committee of a political party'' each place it appears in subparagraphs (A), (B), and (C) and inserting ''committee of a national or State political party''.

(3) STATE PARTY CONVENTION ACCOUNTS DESCRIBED.—Section 315(a) of such Act (52 U.S.C.

30116(a)) is amended by adding at the end the following new paragraph:

"(10) An account described in this paragraph is a separate, segregated account of a political committee established and maintained by a State committee of a political party which is used solely to defray—

"(A) expenses incurred with respect to carrying out State party nominating activities or other party-building conventions; or

"(B) expenses incurred with respect to providing for the attendance of delegates at a presidential nominating convention, but only to the extent that such expenses are not paid for from the account described in paragraph (9)(A).".

(d) CLARIFICATION OF INDEXING OF AMOUNTS TO ENSURE EQUALIZATION OF PARTY CONTRIBUTION LIMITS.—For purposes of applying section 315(c) of such Act (52 U.S.C. 30116(c)) to limits on the amount of contributions to political committees established and maintained by a State political party, the amendments made by this section shall be considered to have been included in section 307 of the Bipartisan Campaign Reform Act of 2002 (Public Law 107–55; 116 Stat. 102).

(e) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 305. EXPANSION OF PERMISSIBLE FEDERAL ELECTION ACTIVITY BY STATE AND LOCAL POLITICAL PARTIES.

(a) EXPANSION OF PERMISSIBLE USE OF FUNDS NOT SUBJECT TO CONTRIBUTION LIMITS OR SOURCE PROHIBITIONS BY STATE AND LOCAL POLITICAL PARTIES FOR FEDERAL ELECTION ACTIVITY.—Section 323(b)(2) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30125(b)(2)) is amended to read as follows:

"(2) APPLICABILITY.—Notwithstanding section 301(20), for purposes of paragraph (1), an amount that is expended or disbursed by a State, district, or local committee of a political party shall be considered to be expended or disbursed for Federal election activity only if the committee coordinated the expenditure or disbursement of the amount with a candidate for election for Federal office or an authorized committee of a candidate for election for Federal office.".

(b) CONFORMING AMENDMENTS.—

(1) FUNDRAISING COSTS.—Section 323(c) of such Act (52 U.S.C. 30125(c)) is amended by add-

ing at the end the following new sentence: ''In the case of a person described in subsection (b), the previous sentence applies only if the amount was spent by such person in coordination with a candidate for election for Federal office or an authorized committee of a candidate for election for Federal office, as determined pursuant to regulations promulgated by the Commission for the purpose of determining whether a political party communication is coordinated with a candidate, a candidate's authorized committee, or an agent thereof.''.

(2) APPEARANCE OF FEDERAL CANDIDATES OR OFFICEHOLDERS AT FUNDRAISING EVENTS.—Section 323(e)(3) of such Act (52 U.S.C. 30125(e)(3)) is amended by striking ''subsection (b)(2)(C)'' and inserting ''subsection (b)''.

SEC. 306. PARTICIPATION IN JOINT FUNDRAISING ACTIVITIES BY MULTIPLE POLITICAL COMMITTEES.

(a) FINDINGS.—Congress finds the following:

(1) While federal law permits the Federal Election Commission to engage in certain ''gap-filling'' activities as it administers the Federal Election Campaign Act of 1971, the regulations promulgated by the Federal Election Commission to govern joint fundraising activities of multiple political committees

are not tied specifically to any particular provision of the Act, and while these regulations generally duplicate the provisions of the Act, they also impose additional and unnecessary burdens on political committees which seek to engage in joint fundraising activities, such as a requirement for written agreements between the participating committees.

(2) It is therefore not necessary at this time to direct the Federal Election Commission to repeal the existing regulations which govern joint fundraising activities of multiple political committees, as some political committees may have reasons for following the provisions of such regulations which impose additional and unnecessary burdens on these activities.

(b) CRITERIA FOR PARTICIPATION IN JOINT FUNDRAISING ACTIVITIES.—Section 302 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30102) is amended by adding at the end the following new subsection:

"(j) CRITERIA FOR PARTICIPATION IN JOINT FUNDRAISING ACTIVITIES BY MULTIPLE POLITICAL COMMITTEES.—

"(1) CRITERIA DESCRIBED.—Two or more political committees as defined in this Act may participate in joint fundraising activities in accordance with the following criteria:

"(A) The costs of the activities shall be allocated among and paid for by the participating committees on the basis of the allocation among the participating committees of the contributions received as a result of the activities.

"(B) Notwithstanding subparagraph (A), a participating committee may make a payment (in whole or in part) for the portion of the costs of the activities which is allocated to another participating committee, and the amount of any such payment shall be treated as a contribution made by the committee to the other participating committee.

"(C) The provisions of section 315(a)(8) regarding the treatment of contributions to a candidate which are earmarked or otherwise directed through an intermediary or conduit shall apply to contributions made by a person to a participating committee which are allocated by the committee to another participating committee.

"(2) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to prohibit two or more political committees from participating in joint fundraising activities by designating or establishing a separate, joint committee subject to the registration and reporting requirements of this Act or by publishing a joint fundraising notice.''.

SEC. 307. PROTECTING PRIVACY OF DONORS TO TAX-EXEMPT ORGANIZATIONS.

(a) SHORT TITLE.—This section may be cited as the ''Speech Privacy Act of 2022''.

(b) RESTRICTIONS ON COLLECTION OF DONOR INFORMATION.—

(1) RESTRICTIONS.—An entity of the Federal government may not collect or require the submission of information on the identification of any donor to a tax-exempt organization.

(2) EXCEPTIONS.—Paragraph (1) does not apply to the following:

(A) The Internal Revenue Service, acting lawfully pursuant to section 6033 of the Internal Revenue Code of 1986 or any successor provision.

(B) The Secretary of the Senate and the Clerk of the House of Representatives, acting lawfully pursuant to section 3 of the Lobbying Disclosure Act of 1995 (2 U.S.C. 1604).

(C) The Federal Election Commission, acting lawfully pursuant to section 510 of title 36, United States Code.

(D) An entity acting pursuant to a lawful order of a court or administrative body which has the authority under law to direct the entity to collect or require the submission of the information, but only to the extent permitted by the lawful order of such court or administrative body.

(c) RESTRICTIONS ON RELEASE OF DONOR INFORMATION.—

(1) RESTRICTIONS.—An entity of the Federal government may not disclose to the public information revealing the identification of any donor to a tax-exempt organization.

(2) EXCEPTIONS.—Paragraph (1) does not apply to the following:

(A) The Internal Revenue Service, acting lawfully pursuant to section 6104 of the Internal Revenue Code of 1986 or any successor provision.

(B) The Secretary of the Senate and the Clerk of the House of Representatives, acting lawfully pursuant to section 3 of the Lobbying Disclosure Act of 1995 (2 U.S.C. 1604).

(C) The Federal Election Commission, acting lawfully pursuant to section 510 of title 36, United States Code.

(D) An entity acting pursuant to a lawful order of a court or administrative body which has the authority under law to direct the entity to disclose the information, but only to the extent permitted by the lawful order of such court or administrative body.

(E) An entity which discloses the information as authorized by the organization.

(d) TAX-EXEMPT ORGANIZATION DEFINED.—In this section, a ‘‘tax-exempt organization'' means an organization which is described in section 501(c) of the Internal Revenue Code of 1986 and is exempt from taxation under section 501(a) of such Code. Nothing in this subsection may be construed to treat a political organization under section 527 of such Code as a tax-exempt organization for purposes of this section.

(e) PENALTIES.—It shall be unlawful for any officer or employee of the United States, or any former officer or employee, willfully to disclose to any person, except as authorized in this section, any information revealing the identification of any donor to a tax-exempt organization. Any violation of this section shall be a felony punishable upon conviction by a fine in any amount not exceeding $250,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

SEC. 308. REPORTING REQUIREMENTS FOR TAX-EXEMPT ORGANIZATIONS.

(a) SHORT TITLE.—This section may be cited as the ‘‘Don’t Weaponize the IRS Act’’.

(b) ORGANIZATIONS EXEMPT FROM REPORTING.—

(1) GROSS RECEIPTS THRESHOLD.—Clause (ii) of section 6033(a)(3)(A) of the Internal Revenue Code of 1986 is amended by striking ‘‘$5,000’’ and inserting ‘‘$50,000’’.

(2) ORGANIZATIONS DESCRIBED.—Subparagraph (C) of section 6033(a)(3) of the Internal Revenue Code of 1986 is amended—

(A) by striking ‘‘and’’ at the end of clause (v),

(B) by striking the period at the end of clause (vi) and inserting a semicolon, and

(C) by adding at the end the following new clauses:

"(vii) any other organization described in section 501(c) (other than a private foundation or a supporting organization described in section 509(a)(3)); and

"(viii) any organization (other than a private foundation or a supporting organization described in section 509(a)(3)) which is not described in section 170(c)(2)(A), or which is created or organized in a possession of the United States, which has no significant activity (including lobbying and political activity and the operation of a trade or business) other than investment activity in the United States.".

(3) EFFECTIVE DATE.—The amendments made by this subsection shall apply to taxable years ending after the date of the enactment of this Act.

(c) CLARIFICATION OF APPLICATION TO SECTION 527 ORGANIZATIONS.—

(1) IN GENERAL.—Paragraph (1) of section 6033(g) of the Internal Revenue Code of 1986 is amended—

(A) by striking ''This section'' and inserting ''Except as otherwise provided by this subsection, this section'', and

(B) by striking ''for the taxable year.'' and inserting ''for the taxable year in the same manner as to an organization exempt from taxation under section 501(a).''.

(2) EFFECTIVE DATE.—The amendments made by this subsection shall apply to taxable years ending after the date of the enactment of this Act.

(d) REPORTING OF NAMES AND ADDRESSES OF CONTRIBUTORS.—

(1) IN GENERAL.—Paragraph (1) of section 6033(a) of the Internal Revenue Code of 1986 is amended by adding at the end the following: ''Except as provided in subsections (b)(5) and (g)(2)(B), such annual return shall not be required to include the names and addresses of contributors to the organization.''.

(2) APPLICATION TO SECTION 527 ORGANIZATIONS.—Paragraph (2) of section 6033(g) of the Internal Revenue Code of 1986 is amended—

(A) by striking ''and'' at the end of subparagraph (A),

(B) by redesignating subparagraph (B) as subparagraph (C), and

(C) by inserting after subparagraph (A) the following new subparagraph:

"(B) containing the names and addresses of all substantial contributors, and".

(3) EFFECTIVE DATE.—The amendments made by this subsection shall apply to taxable years ending after the date of the enactment of this Act.

SEC. 309. MAINTENANCE OF STANDARDS FOR DETERMINING ELIGIBILITY OF SECTION 501(C)(4) ORGANIZATIONS.

(a) IN GENERAL.—The Department of the Treasury, including the Internal Revenue Service, may not issue, revise, or finalize any regulation, revenue ruling, or other guidance not limited to a particular taxpayer relating to the standard which is used to determine whether an organization is operated exclusively for the promotion of social welfare for purposes of section 501(c)(4) of the Internal Revenue Code of 1986 (including the proposed regulations published at 78 Fed. Reg. 71535 (November 29, 2013)).

(b) APPLICATION OF CURRENT STANDARDS AND DEFINITIONS.—The standard and definitions as in effect on January 1, 2010, which are used to make determinations described in subsection (a) shall apply after the date of the enactment of this Act for purposes of determining status under section 501(c)(4) of such Code of organizations created on, before, or after such date.

Subtitle B—Prohibition on Use of Federal Funds for Congressional Campaigns

SEC. 311. PROHIBITING USE OF FEDERAL FUNDS FOR PAYMENTS IN SUPPORT OF CONGRESSIONAL CAMPAIGNS.

No Federal funds, including amounts attributable to the collection of fines and penalties, may be used to make any payment in support of a campaign for election for the office of Senator or Representative in, or Delegate or Resident Commissioner to, the Congress.

Subtitle C—Registration and Reporting Requirements

SEC. 321. REPORTING REQUIREMENTS WITH RESPECT TO ELECTIONEERING COMMUNICATIONS.

Section 304(a)(11)(A)(i) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30104(a)(11)(A)(i)) is amended by inserting ‘‘or makes, or has reason to expect to make, electioneering communications’’ after ‘‘expenditures’’.

SEC. 322. INCREASED QUALIFYING THRESHOLD AND ESTABLISHING PURPOSE FOR POLITICAL COMMITTEES.

(a) IN GENERAL.—Section 301(4) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(4)) is amended to read as follows:

"(4) The term 'political committee' means—

"(A) any committee, club, association, or other group of persons, including any local committee of a political party, which receives contributions aggregating in excess of $25,000 during a calendar year or which makes expenditures aggregating in excess of $25,000 during a calendar year and which is under the control of a candidate or has the major purpose of nominating or electing a candidate; or

"(B) any separate segregated fund established under the provisions of section 316(b).".

(b) DEFINITION.—Section 301 of such Act (52 U.S.C. 30101) is amended by adding at the end the following new paragraph:

"(27) MAJOR PURPOSE OF NOMINATING OR ELECTING A CANDIDATE.—The term 'major purpose of nominating or electing a candidate' means, with respect to a group of persons described in paragraph (4)(A)—

"(A) a group whose central organizational purpose is to expressly advocate for the nomination, election, or defeat of a candidate; or

"(B) a group for which the majority of its spending throughout its lifetime of existence has been on contributions, expenditures, or independent expenditures.".

(c) PRICE INDEX ADJUSTMENT FOR POLITICAL COMMITTEE THRESHOLD.—Section 315(c) of such Act (52 U.S.C. 30116(c)), as amended by section 304(b), is amended—

(1) in paragraph (1), by adding at the end the following new subparagraph:

"(E) In any calendar year after 2022—

"(i) a threshold established by sections 301(4)(A) or 301(4)(C) shall be increased by the percent difference determined under subparagraph (A);

"(ii) each amount so increased shall remain in effect for the calendar year; and

"(iii) if any amount after adjustment under clause (i) is not a multiple of $100, such amount shall be rounded to the nearest multiple of $100."; and

(2) in paragraph (2)(B)—

(A) in clause (ii), by striking "and" at the end;

(B) in clause (iii), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new clause:

"(iv) for purposes of sections 301(4)(A) and 301(4)(C), calendar year 2022.".

(d) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 323. INCREASED THRESHOLD WITH RESPECT TO INDEPENDENT EXPENDITURE REPORTING REQUIREMENT.

(a) IN GENERAL.—Section 304(c)(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30104(c)(1)) is amended by striking "$250" and inserting "$1,000".

(b) PRICE INDEX ADJUSTMENT FOR INDEPENDENT EXPENDITURE REPORTING THRESHOLD.—Section 315(c) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30116(c)), as amended by sections 304(b) and 322(b), is amended—

(1) in paragraph (1), by adding at the end the following new subparagraph:

"(F) In any calendar year after 2022—

''(i) a threshold established by section 304(c)(1) shall be increased by the percent difference determined under subparagraph (A);

''(ii) each amount so increased shall remain in effect for the calendar year; and

''(iii) if any amount after adjustment under clause (i) is not a multiple of $100, such amount shall be rounded to the nearest multiple of $100.''; and

(2) in paragraph (2)(B)—

(A) in clause (iii), by striking ''and'' at the end;

(B) in clause (iv), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following new clause:

''(v) for purposes of section 304(c)(1), calendar year 2022.''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 324. INCREASED QUALIFYING THRESHOLD WITH RESPECT TO CANDIDATES.

(a) INCREASE IN THRESHOLD.—Section 301(2) of the Federal Election Campaign Act of 1971 (52 U.S.C.

30101(2)) is amended by striking "$5,000" each place it appears and inserting "$10,000".

(b) PRICE INDEX ADJUSTMENT FOR EXEMPTION OF CERTAIN AMOUNTS AS CONTRIBUTIONS.—Section 315(c) of such Act (52 U.S.C. 30116(c)), as amended by sections 304(b), 322(b), and 323(b), is amended—

(1) in paragraph (1), by adding at the end the following new subparagraph:

"(G) In any calendar year after 2022—

"(i) a threshold established by sections 301(2) shall be increased by the percent difference determined under subparagraph (A);

"(ii) each amount so increased shall remain for the 2-year period that begins on the first day following the date of the general election in the year preceding the year in which the amount is increased and ending on the date of the next general election; and

"(iii) if any amount after adjustment under clause (i) is not a multiple of $100, such amount shall be rounded to the nearest multiple of $100."; and

(2) in paragraph (2)(B)—

(A) in clause (iv), by striking "and" at the end;

(B) in clause (v), by striking the period at the end and inserting ''; and''; and

(C) by adding at the end the following new clause:

''(vi) for purposes of sections 301(2), calendar year 2022.''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 325. REPEAL REQUIREMENT OF PERSONS MAKING INDEPENDENT EXPENDITURES TO REPORT IDENTIFICATION OF CERTAIN DONORS.

(a) REPEAL.—Section 304(c)(2) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30104(c)(2)) is amended—

(1) in subparagraph (A), by adding ''and'' at the end;

(2) in subparagraph (B), by striking ''; and'' and inserting a period; and

(3) by striking subparagraph (C).

(b) CONFORMING AMENDMENT.—Section 304(c)(1) of such Act (52 U.S.C. 30104(c)(1)) is amended by striking ''the information required under subsection (b)(3)(A) for all contributions received by such person'' and inserting ''the information required under paragraph (2)''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to independent expenditures made on or after the date of the enactment of this Act.

Subtitle D—Exclusion of Certain Amounts From Treatment as Contributions or Expenditures

SEC. 331. INCREASED THRESHOLD FOR EXEMPTION OF CERTAIN AMOUNTS AS CONTRIBUTIONS.

(a) REAL OR PERSONAL PROPERTY EXEMPTION.—Section 301(8)(B)(ii) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(8)(B)(ii)) is amended—

(1) by striking "$1,000" and inserting "$2,000"; and

(2) by striking "$2,000" and inserting "$4,000".

(b) TRAVEL EXPENSES EXEMPTION.—Section 301(8)(B)(iv) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(8)(B)(iv)) is amended—

(1) by striking "$1,000" and inserting "$2,000"; and

(2) by striking "$2,000" and inserting "$4,000".

(c) PRICE INDEX ADJUSTMENT FOR EXEMPTION OF CERTAIN AMOUNTS AS CONTRIBUTIONS.—Section 315(c) of such Act (52 U.S.C. 30116(c)), as amended by sections 304(b), 322(b), 323(b), and 324(b) is amended—

(1) in paragraph (1), by adding at the end the following new subparagraph:

"(H) In any calendar year after 2022—

"(i) the exemption amounts established by sections 301(8)(B)(ii) or 301(8)(B)(iv) shall be increased by the percent difference determined under subparagraph (A);

"(ii) each amount so increased shall remain for the 2-year period that begins on the first day following the date of the general election in the year preceding the year in which the amount is increased and ending on the date of the next general election; and

"(iii) if any amount after adjustment under clause (i) is not a multiple of $100, such amount shall be rounded to the nearest multiple of $100."; and

(2) in paragraph (2)(B)—

(A) in clause (v), by striking "and" at the end;

(B) in clause (vi), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following new clause:

"(vii) for purposes of sections 301(8)(B)(ii) or 301(8)(B)(iv), calendar year 2022.".

(d) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 332. EXEMPTION OF UNCOMPENSATED INTERNET COMMUNICATIONS FROM TREATMENT AS CONTRIBUTION OR EXPENDITURE.

(a) EXEMPTIONS.—

(1) EXEMPTION FROM TREATMENT AS CONTRIBUTION.—Section 301(8)(B) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(8)(B)) is amended—

(A) by striking "and" at the end of clause (xiii);

(B) by striking the period at the end of clause (xiv) and inserting "; and"; and

(C) by adding at the end the following new clause:

"(xv) any payment by any person in producing and disseminating any information or communication on the Internet, Internet platform or other

Internet-enabled application, unless the information or communication is disseminated for a fee on another person's website, platform or other Internet-enabled application, whether coordinated or not.''.

(2) EXEMPTION FROM TREATMENT AS EXPENDITURE.—Section 301(9)(B) of such Act (52 U.S.C. 30101(9)(B)) is amended—

(A) by striking ''and'' at the end of clause (ix);

(B) by striking the period at the end of clause (x) and inserting ''; and''; and

(C) by adding at the end the following new clause:

''(xi) any cost incurred by any person in producing and disseminating any information or communication on the Internet, Internet platform or other Internet-enabled application, unless the information or communication is disseminated for a fee on another person's website, platform or other Internet-enabled application.''.

(b) APPLICATION TO DEFINITION OF PUBLIC COMMUNICATIONS.—Section 301(22) of such Act (52 U.S.C. 30101(22)) is amended by adding at the end the following: ''In the previous sentence, the terms 'public communication' and 'general public political advertising' do not include communications disseminated over the Internet or via an Internet platform or other Internet-enabled application, unless the communication or advertising is disseminated for a fee on another person's website, platform or other internet-enabled application.''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

SEC. 333. MEDIA EXEMPTION.

(a) EXPANSION OF EXEMPTION TO ADDITIONAL FORMS OF MEDIA.—Section 301(9)(B)(i) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(9)(B)(i)) is amended to read as follows:

> ''(i) any news story, commentary, or editorial distributed through the facilities of any broadcasting, cable, satellite, or internet-based station, programmer, operator or producer; newspaper, magazine, or other periodical publisher; electronic publisher, platform, or application; book publisher; or filmmaker or film producer, distributor or exhibitor, unless such facilities are owned or controlled by any political party, political committee, or candidate;''.

(b) APPLICATION TO CONTRIBUTIONS.—Section 301(8)(B) of such Act (52 U.S.C. 30101(8)(B)), as amended by section 332(a)(1), is amended—

(1) by redesignating clauses (i) through (xv) as clauses (ii) through (xvi); and

(2) by inserting before clause (ii) (as so redesignated) the following new clause:

"(i) any payment for any news story, commentary, or editorial distributed through the facilities of any broadcasting, cable, satellite, or internet-based station, programmer, operator or producer; newspaper, magazine, or other periodical publisher; electronic publisher, platform, or application; book publisher; or filmmaker or film producer, distributor or exhibitor.".

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to elections held during 2024 or any succeeding year.

Subtitle E—Prohibition on Issuance of Regulations on Political Contributions

SEC. 341. PROHIBITION ON ISSUANCE OF REGULATIONS ON POLITICAL CONTRIBUTIONS.

The Securities and Exchange Commission may not finalize, issue, or implement any rule, regulation, or order regarding the disclosure of political contributions, contributions to tax exempt organizations, or dues paid to trade associations.

Subtitle F—Miscellaneous Provisions

SEC. 351. PERMANENT EXTENSION OF FINES FOR QUALIFIED DISCLOSURE REQUIREMENT VIOLATIONS.

Section 309(a)(4)(C)(v) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30109(a)(4)(C)(v)) is amended by striking ‘‘, and that end on or before December 31, 2023’’.

SEC. 352. POLITICAL COMMITTEE DISBURSEMENT REQUIREMENTS.

Section 302(h)(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30102(h)(1)) is amended by striking ‘‘except by check drawn on such accounts in accordance with this section’’ and inserting ‘‘except from such accounts’’.

SEC. 353. DESIGNATION OF INDIVIDUAL AUTHORIZED TO MAKE CAMPAIGN COMMITTEE DISBURSEMENTS IN EVENT OF DEATH OF CANDIDATE.

(a) IN GENERAL.—Section 302 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30102), as amended by section 307(b), is amended by adding at the end the following new subsection:

"(k)(1) Each candidate may, with respect to each authorized committee of the candidate, designate an individual who shall be responsible for disbursing funds in the accounts of the committee in the event of the death of the candidate, and may also designate another individual to carry out the responsibilities of the designated individual under this subsection in the event of the death or incapacity of the designated individual or the unwillingness of the designated individual to carry out the responsibilities.

"(2) In order to designate an individual under this subsection, the candidate shall file with the Commission a signed written statement (in a standardized form developed by the Commission) that contains the name and address of the individual and the name of the authorized committee for which the designation shall apply, and that may contain the candidate's instructions regarding the disbursement of the funds involved by the individual. At any time after filing the statement, the candidate may revoke the designation of an individual by filing with the Commission a signed written statement of revocation (in a standardized form developed by the Commission).

"(3)(A) Upon the death of a candidate who has designated an individual for purposes of paragraph (1), funds in the accounts of each authorized committee of the candidate may be disbursed only under the direction and in accordance with the instructions of such individual, subject to the terms and conditions applicable to the disbursement of such funds under this Act or any other applicable Federal or State law (other than any provision of State law which authorizes any person other than such individual to direct the disbursement of such funds).

"(B) Subparagraph (A) does not apply with respect to an authorized committee if, at the time of the candidate's death, the authorized committee has a treasurer or a designated agent of the treasurer as described in section 302(a), unless the treasurer or designated agent is incapacitated or cannot be reached by the authorized committee.

"(C) Nothing in this paragraph may be construed to grant any authority to an individual who is designated pursuant to this subsection other than the authority to direct the disbursement of funds as provided in such paragraph, or may be construed to affect the responsibility of the treasurer of an authorized committee for which funds are disbursed in accordance with such paragraph to file reports of the disbursements of such funds under section 304(a).''.

(b) Inclusion of Designation in Statement of Organization of Committee.—Section 303(b) of such Act (52 U.S.C. 30103(b)) is amended—

(1) in paragraph (5), by striking ''and'' at the end;

(2) in paragraph (6), by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following new paragraph:

''(7) in the case of an authorized committee of a candidate who has designated an individual under section 302(k) (including a second individual designated to carry out the responsibilities of that individual under such section in the event of that individual's death or incapacity or unwillingness to carry out the responsibilities) to disburse funds from the accounts of the committee in the event of the death of the candidate, a copy of the statement filed by the candidate with the Commission under such section (as well as a copy of any subsequent statement of revocation filed by the candidate with the Commission under such section).''.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to authorized campaign committees which are designated under section 302(e)(1) of the Federal Election Campaign Act of 1971 before, on, or after the date of the enactment of this Act.

SEC. 354. PROHIBITION ON CONTRIBUTIONS IN NAME OF ANOTHER.

Section 320 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30122) is amended by adding at the end the following new sentence: ‘‘No person shall knowingly direct, help, or assist any person in making a contribution in the name of another person.’’.

SEC. 355. UNANIMOUS CONSENT OF COMMISSION MEMBERS REQUIRED FOR COMMISSION TO REFUSE TO DEFEND ACTIONS BROUGHT AGAINST COMMISSION.

(a) UNANIMOUS CONSENT.—Section 307 of the Federal Election Campaign Act of 1971 (52 U.S.C. 30107) is amended by adding at the end the following new subsection:

‘‘(f)(1) Except as provided in paragraph (2), the Commission shall defend each action brought against the Commission under this Act or chapter 95 and 96 of the Internal Revenue Code of 1986—

"(A) through the general counsel, as provided in subsection (a)(6);

"(B) by appointing counsel as provided in section 306(f)(4); or

"(C) by referral to the Attorney General in the case of a criminal action.

"(2) The Commission may refuse to defend an action brought against the Commission pursuant to the unanimous vote of its Members.".

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to actions brought on or after the date of the enactment of this Act.

SEC. 356. FEDERAL ELECTION COMMISSION MEMBER PAY.

Section 306(a)(4) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30106(a)(4)) is amended by striking "equivalent to the compensation paid at level IV of the Executive Schedule (5 U.S.C. 5315)" and inserting "at an annual rate of basic pay of $186,300, as adjusted under section 5318 of title 5, United States Code, in the same manner as the annual rate of pay for positions at each level of the Executive Schedule".

SEC. 357. UNIFORM STATUTE OF LIMITATIONS FOR PROCEEDINGS TO ENFORCE FEDERAL ELECTION CAMPAIGN ACT OF 1971.

(a) 5-YEAR LIMITATION.—Section 406(a) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30145(a)) is amended—

(1) by striking "(a)" and inserting "(a)(1)"; and

(2) by adding at the end the following new paragraph:

"(2) No person shall be subject to a civil penalty for any violation of title III of this Act unless the proceeding is initiated in accordance with section 309 not later than 5 years after the date on which the violation occurred.".

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to violations occurring on or after the date of the enactment of this Act.

SEC. 358. THEFT FROM POLITICAL COMMITTEE AS A FEDERAL CRIME.

(a) FEDERAL CRIME.—Chapter 29 of title 18, United States Code, as amended by section 161(b), is amended by adding at the end the following new section:

"§ 613. Theft from political committee

"(a) IN GENERAL.—It shall be unlawful... [*policy to be provided, including whether this applies only to Federal committees or to State and local campaigns as well (i.e.,* *perhaps referring to political organizations under 527 of the IRC?)*]

"(b) PENALTY.—Any person who violates subsection (a) shall be fined not more than $____________________, imprisoned for not more than _______________, or both.".

(b) CLERICAL AMENDMENT.—The table of sections for chapter 28 of title 18, United States Code, is amended by adding at the end the following new item:

"613. Theft from political committee.".

SEC. 359. DEADLINE FOR PROMULGATION OF PROPOSED REGULATIONS.

Not later than 120 days after the date of the enactment of this Act, the Federal Election Commission shall publish in the Federal Register proposed regulations to carry out this title and the amendments made by this title.

TITLE IV—ELECTION SECURITY

Subtitle A—Promoting Election Security

SEC. 401. SHORT TITLE.

This title may be cited as the "Election Security Assistance Act".

SEC. 402. REPORTS TO CONGRESS ON FOREIGN THREATS TO ELECTIONS.

(a) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, and 30 days after the end of each fiscal year thereafter, the Secretary of Homeland

Security and the Director of National Intelligence, in coordination with the heads of the appropriate Federal entities, shall submit a joint report to the appropriate congressional committees and the chief State election official of each State on foreign threats to elections in the United States, including physical and cybersecurity threats.

(b) VOLUNTARY PARTICIPATION BY STATES.—The Secretary shall solicit and consider voluntary comments from all State election agencies. Participation by an election agency in the report under this section shall be voluntary and at the discretion of the State.

(c) APPROPRIATE FEDERAL ENTITIES.—In this section, the term ‘‘appropriate Federal entities'' means—

(1) the Department of Commerce, including the National Institute of Standards and Technology;

(2) the Department of Defense;

(3) the Department of Homeland Security, including the component of the Department that reports to the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department;

(4) the Department of Justice, including the Federal Bureau of Investigation;

(5) the Election Assistance Commission; and

(6) the Office of the Director of National Intelligence, the National Security Agency, and such other elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) as the Director of National Intelligence determines are appropriate.

(d) OTHER DEFINITIONS.—In this section—

(1) the term ''appropriate congressional committees'' means—

(A) the Committee on Rules and Administration, the Committee on Homeland Security and Governmental Affairs, the Select Committee on Intelligence, and the Committee on Foreign Relations of the Senate; and

(B) the Committee on House Administration, the Committee on Homeland Security, the Permanent Select Committee on Intelligence, and the Committee on Foreign Affairs of the House of Representatives;

(2) the term ''chief State election official'' means, with respect to a State, the individual designated by the State under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509) to be responsible for coordination of the State's responsibilities under such Act;

(3) the term ''election agency'' means any component of a State or any component of a unit of local government of a State that is responsible for administering Federal elections;

(4) the term ''Secretary'' means the Secretary of Homeland Security; and

(5) the term ''State'' has the meaning given such term in section 901 of the Help America Vote Act of 2002 (52 U.S.C. 21141).

SEC. 403. RULE OF CONSTRUCTION.

Nothing in this title may be construed as authorizing the Secretary of Homeland Security to carry out the administration of an election for Federal office.

Subtitle B—Cybersecurity for Election Systems

SEC. 411. CYBERSECURITY ADVISORIES RELATING TO ELECTION SYSTEMS.

(a) CYBERSECURITY ADVISORIES.—

(1) IN GENERAL.—The Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security (in this subtitle referred to as the ''Director'') shall collaborate with the Election Assistance Commission (in this subtitle referred to as the ''Commission'') to determine if an advisory relating to the cybersecurity of election sys-

tems used in the administration of elections for Federal office or the cybersecurity of elections for Federal office generally is necessary. If such a determination is made in the affirmative, the Director shall collaborate with the Commission in the preparation of such an advisory.

(2) PROHIBITION.—The Director may not issue an advisory described in paragraph (1) unless the Commission has provided input relating thereto.

(b) NOTIFICATION.—If the Director issues an advisory described in subsection (a), the Director, in collaboration with the Commission, shall provide to appropriate State election officials and vendors of covered voting systems notification relating thereto.

SEC. 412. PROCESS TO TEST FOR AND MONITOR CYBERSECURITY VULNERABILITIES IN ELECTION EQUIPMENT.

(a) PROCESS FOR COVERED VOTING SYSTEMS.—

(1) IN GENERAL.—The Director and the Commission (in consultation with the Technical Guidelines Development Committee and the Standards Board of the Commission), shall jointly establish a voluntary process to test for and monitor covered voting systems for cybersecurity vulnerabilities. Such process shall include the following:

(A) Mitigation strategies and other remedies.

(B) Notice to the Commission and appropriate entities of the results of testing conducted pursuant to such process.

(2) IMPLEMENTATION.—The Director shall implement the process established under paragraph (1) at the request of the Commission.

(b) LABELING FOR VOTING SYSTEMS.—The Commission (in consultation with the Technical Guidelines Development Committee and the Standards Board of the Commission), shall establish a process to provide for the deployment of appropriate labeling available through the website of the Commission to indicate that covered voting systems passed the most recent cybersecurity testing pursuant to the process established under subsection (a).

(c) RULES OF CONSTRUCTION.—The process established under subsection (a), including the results of any testing carried out pursuant to this section, shall not affect—

(1) the certification status of equipment used in the administration of an election for Federal office under the Help America Vote Act of 2002; or

(2) the authority of the Commission to so certify such equipment under such Act.

(d) DEFINITION.—In this section, the term ''covered voting systems'' means equipment used in the administration of an election for Federal office that is certified in accordance with versions of Voluntary Voting System Guidelines under the Help America Vote Act of 2002 under which such equipment is not required to be tested for cybersecurity vulnerabilities.

SEC. 413. DUTY OF SECRETARY OF HOMELAND SECURITY TO NOTIFY STATE AND LOCAL OFFICIALS OF ELECTION CYBERSECURITY INCIDENTS.

(a) DUTY TO SHARE INFORMATION WITH DEPARTMENT OF HOMELAND SECURITY.—If a Federal entity receives information about an election cybersecurity incident, the Federal entity shall promptly share that information with the Department of Homeland Security, unless the head of the entity (or a Senate-confirmed official designated by the head) makes a specific determination in writing that there is good cause to withhold the particular information.

(b) RESPONSE TO RECEIPT OF INFORMATION BY SECRETARY OF HOMELAND SECURITY.—

(1) IN GENERAL.—Upon receiving information about an election cybersecurity incident under subsection (a), the Secretary of Homeland Security, in consultation with the Attorney General, the Director

of the Federal Bureau of Investigation, and the Director of National Intelligence, shall promptly (but in no case later than 96 hours after receiving the information) review the information and make a determination whether each of the following apply:

(A) There is credible evidence that the incident occurred.

(B) There is a basis to believe that the incident resulted, could have resulted, or could result in voter information systems or voter tabulation systems being altered or otherwise affected.

(2) DUTY TO NOTIFY STATE AND LOCAL OFFICIALS.—

(A) DUTY DESCRIBED.—If the Secretary makes a determination under paragraph (1) that subparagraphs (A) and (B) of such paragraph apply with respect to an election cybersecurity incident, not later than 96 hours after making the determination, the Secretary shall provide a notification of the incident to each of the following:

(i) The chief executive of the State involved.

(ii) The State election official of the State involved.

(iii) The local election official of the election agency involved.

(B) Treatment of classified information.—

(i) Efforts to avoid inclusion of classified information.—In preparing a notification provided under this paragraph to an individual described in clause (i), (ii), or (iii) of subparagraph (A), the Secretary shall attempt to avoid the inclusion of classified information.

(ii) Providing guidance to State and local officials.—To the extent that a notification provided under this paragraph to an individual described in clause (i), (ii), or (iii) of subparagraph (A) includes classified information, the Secretary (in consultation with the Attorney General and the Director of National Intelligence) shall indicate in the notification which information is classified.

(3) Exception.—

(A) IN GENERAL.—If the Secretary, in consultation with the Attorney General and the Director of National Intelligence, makes a determination that it is not possible to provide a notification under paragraph (1) with respect to an election cybersecurity incident without compromising intelligence methods or sources or interfering with an ongoing investigation, the Secretary shall not provide the notification under such paragraph.

(B) ONGOING REVIEW.—Not later than 30 days after making a determination under subparagraph (A) and every 30 days thereafter, the Secretary shall review the determination. If, after reviewing the determination, the Secretary makes a revised determination that it is possible to provide a notification under paragraph (2) without compromising intelligence methods or sources or interfering with an ongoing investigation, the Secretary shall provide the notification under paragraph (2) not later than 96 hours after making such revised determination.

(4) COORDINATION WITH ELECTION ASSISTANCE COMMISSION.—The Secretary shall make determinations and provide notifications under this

subsection in the same manner, and subject to the same terms and conditions relating to the role of the Election Assistance Commission, in which the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security makes determinations as to the necessity of an advisory and the issuance of an advisory under section 411(a) and the provision of notification under section 411(b).

(c) DEFINITIONS.—In this section, the following definitions apply:

(1) ELECTION AGENCY.—The term ‘‘election agency’’ means any component of a State, or any component of a unit of local government in a State, which is responsible for the administration of elections for Federal office in the State.

(2) ELECTION CYBERSECURITY INCIDENT.— The term ‘‘election cybersecurity incident’’ means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system of election infrastructure (including a vote tabulation system), or actually or imminently jeopardizes, without lawful authority, such an information system of election infrastructure.

(3) FEDERAL ELECTION.—The term ''Federal election'' means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1))) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3))).

(4) FEDERAL ENTITY.—The term ''Federal entity'' means any agency (as defined in section 551 of title 5, United States Code).

(5) LOCAL ELECTION OFFICIAL.—The term ''local election official'' means the chief election official of a component of a unit of local government of a State that is responsible for administering Federal elections.

(6) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(7) STATE.—The term ''State'' means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of Northern Mariana Islands, and the United States Virgin Islands.

(8) STATE ELECTION OFFICIAL.—The term ''State election official'' means—

(A) the chief State election official of a State designated under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509); or

(B) in the case of Puerto Rico, Guam, American Samoa, the Northern Mariana Islands, and the United States Virgin Islands, a chief State election official designated by the State for purposes of this Act.

(d) EFFECTIVE DATE.—This section shall apply with respect to information about an election cybersecurity incident which is received on or after the date of the enactment of this Act.

TITLE V—SENSE OF CONGRESS WITH RESPECT TO ROLE OF STATES IN CONGRESSIONAL REDISTRICTING

SEC. 501. SENSE OF CONGRESS WITH RESPECT TO ROLE OF STATES IN CONGRESSIONAL REDISTRICTING.

It is the sense of Congress that, while Congress is authorized under the Constitution of the United States to ensure that congressional redistricting is carried out in a manner consistent with the Constitution, only a State has the authority to establish maps of the congressional districts of the State and to determine the procedures and criteria used to establish such maps.

TITLE VI—DISINFORMATION GOVERNANCE BOARD

SEC. 601. TERMINATION OF THE DISINFORMATION GOVERNANCE BOARD.

The Disinformation Governance Board of the Department of Homeland Security is hereby terminated.

SEC. 602. PROHIBITION ON FUNDING THE ACTIVITIES OF THE DISINFORMATION GOVERNANCE BOARD.

No Federal funds authorized to be appropriated or otherwise made available may be used to establish or carry out the activities of any other entity that is substantially similar to the Disinformation Governance Board terminated by section 701.

TITLE VII—SEVERABILITY

SEC. 701. SEVERABILITY.

If any provision of this Act or any amendment made by this Act, or the application of any such provision or amendment to any person or circumstance, is held to be unconstitutional, the remainder of this Act, and the application of such provision or amendment to any other person or circumstance, shall not be affected by the holding.

AMERICAN CONFIDENCE IN ELECTIONS ACT

Educate. Engage. Reform.

American Confidence in Elections Act (ACE Act)

Summary: The *American Confidence in Elections Act* (ACE Act) is the key Republican election integrity bill now that we are in the Majority. It focuses on the importance of strong election integrity reforms that meet the moment by bolstering voter confidence in our elections while respecting the Constitution, federalism, and conservative principles. Further, the ACE Act continues to address disappointing challenges faced by military and overseas voters and makes the biggest legislative effort in a generation to protect political speech in a climate where Democrats are doing everything in their power to determine "truth" and silence conservative voices.

General Findings

- States have the primary role in establishing election law and administering elections.
- All eligible voters must be able to vote, and all lawful votes must be counted.
- Political speech is protected speech and all voices must be protected.
- Includes the Committee's report on the constitutional role of the states and Congress in election regulation.

Title I – Election Integrity and Voter Confidence

Providing States with the Tools to Bolster Voter Confidence and Improve Election Integrity

- General findings that explain Congress' proper role under the Constitution.
- Establishes with the existing bipartisan Election Assistance Commission (EAC) Standards Board and Local Leadership Council a federal forum for states to share best practices and discuss successes and failures so that all may benefit from innovation and lessons learned across the country. The forum will create no binding recommendations but will release records of its conversations in the form of voluntary considerations on the following topics: the process for the administration of ballots delivered by mail, signature verification procedures, voter list maintenance, access for election observers, timely reporting of the results of ballot counting, recruiting poll workers, public education with respect to the certification and testing of voter machines prior to elections, post-election audits, and secure chain of custody procedures for ballots and election equipment.
- Directs the EAC to develop voluntary guidelines for the use of nonvoting election technology like electronic poll books.
- Establishes the EAC as the lead federal agency on all election administration matters and grants the agency exclusive authority to make election administration grant disbursements to states.
- Requires the National Institute of Science and Technology to provide status reports to Congress on its responsibilities under the *Help America Vote Act* (HAVA).
- Confirms that States must provide access for congressional election observers under Congress' constitutional role to serve as the "Judge of the Elections, Returns and Qualifications of its own Members[.]"
- Requires the USPS to prioritize election mail and mark all election mail with the date of receipt, and process and deliver election mail even if the election officials' account is underfunded or overdrawn. Allows the USPS to recoup any such costs in arrears. Adds criminal penalties for forging a postmark. (Massie Amendment)
- Allows national, state, and local political committees to use the non-profit rate for the purpose of cooperative mailings.
- Requires the USPS to coordinate with states to identify and assign a mailing address to each home in every state, including those residences on Native American land. (Cole)
- Amends the IRS code by allowing certain compensation of election workers to be excluded from gross income and removes the federal requirement that elections officials issue 1099 or W-2 forms to election workers, eliminating a major administrative burden.
- Expressly allows states to use HAVA dollars to conduct post-election audits.
- Requires any public communications paid for by HAVA dollars to contain a disclaimer.
- Allows states to provide preference to veterans and individuals with disabilities when hiring election workers.
- Disincentives "collusive" settlements by requiring SCOTUS to hear an appeal in any case that invalidates a state statute on federal constitutional grounds. (Repeals 1988 Biden law change)
- Clarifies that election materials that must be preserved for 22 months pursuant to HAVA include ballot envelopes of voted ballots only.
- Clarifies federal agency involvement in voter registration by establishing that Executive Order 14019 (Biden election executive order) shall have no force (except as may otherwise be required by law).
- Includes the *Promoting Free and Fair Elections Act* which prohibits federal agencies from engaging in voter registration/mobilization activities and requires agencies that submitted a plan for promoting voter registration under E.O. 14019 to give it to Congress. (H.R. 3072, Tenney)
- Prohibits the use of federal funds by states to administer elections for federal office unless the state imposes certain restrictions on ballot harvesting and the transmission of mail ballots.
- Establishes a bipartisan panel to recommend to Congress model legislation providing for an appropriate process to resolve any vacancy created by the death of a candidate in a contingent presidential or vice-presidential elect. (H.R. 4638, *Solving an Overlooked Loophole in Votes for Executives* (SOLVE) Act, 117th Congress, Davis, Spanberger, A. King, Portman)

Preventing Non-Citizens from Participating in Our Elections

- Clarifies that states have the authority to remove non-citizens from their federal voter registration lists under their regular voter list maintenance programs.
- Expressly restates that it is a felony for non-citizens to vote in federal elections.
- Penalizes states that allow non-citizen voting in state or local elections by reducing the share of new HAVA grant funds by 30%.
- Prohibits states from maintaining a single voter registration roll for state and Federal elections if the state permits non-citizens to vote in state and local elections. Prohibits states from using federal dollars to build or maintain a state-specific roll containing non-citizens.
- Requires states that allow non-citizen voting to have separate ballots for local races if the election occurs during a federal election and prohibits federal dollars to create ballots for non-citizens.
- Requires federal courts to notify the chief state election official and attorney general when non-citizens are excused from jury duty so that states may update their voter rolls. Requires election officials to coordinate their registration rolls with federal court jury lists.
- Prohibits foreign nationals from making financial or in-kind contributions in connection with state or local ballot initiatives or referendums and adds criminal penalties for doing so.
- Requires states to include with their existing biannual reports to the EAC the total number of inactive registrants and the number of registrants removed from the list of official voters. (Palmer)
- Allows a state's proof of citizenship requirement to be included in the state instructions on the national mail voter registration form maintained by EAC. (H.R. 8528, *State Instruction Inclusion Act*, 117th Congress, Palmer)

Other List Maintenance Provisions

- Subject to privacy considerations, requires federal agencies upon state request to share relevant information with state agencies for list maintenance and voter registration purposes.

Voter Identification

- Modernizes the existing HAVA first-time mail voter ID requirement to include all first-time voter registrations made using any method other than in-person at an elections office or state voter registration agency. Also requires certain voters who request a mail ballot or vote by mail to provide HAVA ID.
- Reforms the REAL ID Act to require "CITIZEN" to be printed on all qualifying individuals' identification documents issued or renewed after January 1, 2026.
- Recognizes REAL ID identification documents as appropriate for photographic voter identification, as recommended by the Carter-Baker Commission.

Ending Private Funding for Election Administration

- Includes the *End Zuckerbucks Act* which removes the federal tax exemption for direct, indirect, below-cost services, scholarships, subsidies, or other private funding for election administration. (H.R 1725, Tenney)

Requiring D.C., Which Congress Controls, to Implement Election Integrity and Voter Confidence Measures

- In addition to the above, this bill implements in the District of Columbia the *American Confidence in Elections: D.C. Election Integrity and Voter Confidence Act*, which would serve as an example to the States of effective election administration. It includes:
    - a requirement for all voters to present a photo ID to vote in person or to request an absentee/mail ballot. It also requires D.C. to provide a free copy of the voter's ID and include photos or digital images of registered voters in the poll books with measures in place to protect privacy;
    - a requirement that voter roll list maintenance be conducted annually and a prohibition on same-day registration;
    - a prohibition on ballot harvesting (H.R. 6882, *Election Fraud Prevention Act*, 116th Congress, Davis) and certain restrictions on the use of ballot drop boxes;
    - a prohibition on mailing ballots except upon voter's request;
    - a prohibition on non-citizen voting;
    - a requirement for meaningful observer access;
    - a requirement for a signature verification process for mail ballots and a requirement for signatures to be dated;
    - a requirement that all ballots except military/overseas ballots be received by the close of polls and that election officials report unofficial results no later than 10:00 a.m. the following day;
    - a requirement that after the closing of polls on the date of a D.C. election, the District makes available on a publicly accessible website the total number of voted ballots in the possession of election officials as of the time of the closing of polls (Donalds) and publish the total number of *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA) ballots requested and received, including UOCAVA ballots received that may have been sent pursuant to law without a request.
    - a requirement that D.C. officials ensure that all election administration activities are carried out in a bipartisan manner;
    - a requirement that provisional ballots only be counted when cast in the correct precinct; and
    - a requirement that an audit be conducted following each election before the time to contest the election expires.

<u>Title II – Military Voting Administration</u>

- Directs GAO to conduct a study on voting access for absent uniformed services voters.

Title III – Protecting Political Speech and Campaign Finance Reform

- Repeals limits on coordinated political party expenditures, allowing party committees to work directly with candidates without current restrictions that require the use of IE units, hybrid advertisements, and other methods.
- Allows two or more political committees to participate in joint fundraising activities without the hassle of establishing a joint fundraising agreement or a separate joint committee (but maintains existing formal requirements as an option).
- Raises contribution limits for state political party committees and allows the establishment of higher-limit building, legal, and convention funds as used by the national party committees and indexes limits for inflation.
- Increases qualifying threshold for political committees, candidate committees, and independent expenditure reporting requirements and indexes for inflation.
- Increases "at-home" event exemption amounts and indexes for inflation.
- Excludes certain costs related to party committee and candidate communications soliciting funds from treatment as contributions or expenditures.
- Prohibits the use of federal funds in support of congressional campaigns. (H.R. 4261, 116th Congress, Davis)
- Codifies existing donor disclosure protections for certain tax-exempt organizations. (*NAACP v. Alabama* and *AFPF v. Bonta*)
- Removes statutory limits on aggregate individual contributions, which SCOTUS struck down in 2014. (McCutcheon v. FEC)
- Makes permanent the FEC's alternative dispute resolution process, which had been extended on a temporary basis.
- Includes H.R.149 (114th Congress), which would permit candidates to name individuals who could disperse the funds of a federal campaign committee in accordance with the law in the event of a candidate's death.
- Codifies the existing regulatory prohibition on making political contributions in the name of another person.
- Increases from $5,000 to $50,000 the gross receipts threshold used to determine the eligibility of tax-exempt organizations for the exemption from certain disclosure and reporting requirements. (S. 1105, *Don't Weaponize the IRS Act*, M. Kelly, McConnell, Braun, Cassidy)
- Directs the Department of the Treasury to not issue, revise, or finalize any regulation revenue ruling, or other guidance not limited to a particular taxpayer relating to the standard which is used to determine whether an organization is operated exclusively for the promotion of social welfare for purposes of Section 501(c)(4) of the Internal Revenue Code.
- Modernizes reporting requirements for electioneering communications.
- Modernizes threshold amount and establishes a price index adjustment for political committee threshold.
- Repeals the requirement of persons making independent expenditures to report the identification of certain donors.
- Increases the threshold limits for the real or personal property exemption and the travel expenses exemption and then indexes them for inflation.
- Exempts any payment for information or communication on the internet as a contribution unless it is disseminated for a fee on another person's website and expands the existing media exemption.
- Prohibits the Securities and Exchange Commission from issuing regulations regarding the disclosure of political contributions, contributions to tax-exempt organizations, or dues paid to trade associations.
- Requires unanimous consent of FEC Commissioners to decline to defend an action against the agency.
- Establishes a 5-year statute of limitations for all violations of the *Federal Election Campaign Act* of 1971.

Title IV – Election Security

- Directs the U.S. Department of Homeland Security (DHS) and the Director of National Intelligence to report on physical and cybersecurity threats to elections to Congress and the chief state election official of each state.
- Directs the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the EAC, to determine if an elections-related cybersecurity advisory should be issued.
- Directs CISA, in collaboration with the Technical Guidelines Development Committee and the Standards Board of the EAC, to establish a voluntary process to test for and monitor covered voting systems for cybersecurity vulnerabilities.
- Directs any Federal entity that receives information about an election cybersecurity incident to promptly inform DHS.
- Requires DHS to notify state and local officials of election cybersecurity incidents and collaborate with the EAC for the development and release of any cybersecurity advisories.

Title V – Sense of Congress with Respect to the Role of State Legislatures in Congressional Redistricting

- Congress plays a very limited role in congressional redistricting, ensuring that states carry out the process consistent with the Constitution.
- States are best situated—and constitutionally hold the power—to determine the best redistricting methods in their jurisdictions.

Title VI – Disinformation Governance Board

- Terminates the Disinformation Governance Board at DHS and prevents the use of funds to establish the Disinformation Governance Board or any board similar in nature.

Questions? Contact Caleb Hays, Committee on House Administration Republican General Counsel & Deputy Staff Director, at Caleb.Hays@mail.house.gov.

From: Keith Ingram
To: Christina Adkins; Kristi Hart; Adam Bitter
Subject: Fwd: Texas''s Voter Information Comparison with Experian's True Trace Solution
Date: Friday, June 9, 2023 11:56:46 AM

Get Outlook for iOS

From: Delilah Moreno <[redacted]
Sent: Friday, June 9, 2023 11:55
To: Keith Ingram <KIngram@sos.texas.gov>
Subject: Texas's Voter Information Comparison with Experian's True Trace Solution

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hi Keith, I hope you are doing well sir. I read recently that Texas withdrew from ERIC. I'm not sure how this has impacted your mailing and list maintenance strategies, but I'm sure you and the team are working on a plan to help the state of Texas and possibly other states as well.

Experian is here to help, whether it's just a simple batch delivery for the state of Texas to enhance the process you are building to even a batch by county level. Texas and or counties can perform a Voter Information Comparison with Experian's True Trace Solution with just (at minimum) Name and Address. No Social Security number or Driver License Number is needed to perform the comparison. Experian's Voter Information Comparison via True Trace allows any jurisdiction to compare their voter registration for any state or county list, please see the benefits below.

The benefits of this solution include:

- Running a comparison to Every State regardless of whether they are part of the consortium you are using, for example California, Alabama, West Virginia, Texas – ALL States are on our comparison list.
- Fresh Vetted Data sources that are updated daily, weekly (every 7 days) and monthly (30 days), saving you delays due to undeliverable mail
- High address location accuracy with minimal false positives
- Three methods of delivery:
    - Flexible Batch delivery (great for large volumes of records)
    - Real time Web Portal (great for manual searches)
    - Real Time Web Services (a program connectivity for existing software)
- No Set Up fees for Batch or Web Portal

Keith, please let me know when you are free next week to discuss your plan of action to help the State of Texas and what you need from Experian to help you get there. Please share your availability and I will do my best to accommodate your schedule.

You can reach me at delilah.moreno@experian.com, 512-769-9735 or I can stop by your office as well.

Thank you,
Delilah Moreno

From: Christina Adkins
To: Adam Bitter; Kristi Hart
Subject: FW: Invitation - Orange County, CA Presentation on Experian"s Voter List Maintenance Tool
Date: Wednesday, September 13, 2023 12:37:41 PM

FYI --

From: Kimberly Smith <KSmith@eac.gov>
Sent: Tuesday, September 12, 2023 11:03 AM
To: Kimberly Smith <KSmith@eac.gov>
Cc: Adam Thomas <AThomas@eac.gov>
Subject: Invitation - Orange County, CA Presentation on Experian's Voter List Maintenance Tool

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Standards Board Members,

On behalf of DFO Commissioner Hicks, the EAC would like to invite you to attend a presentation co-hosted by Orange County, California and Experian about using Experian's tool for Voter List Maintenance on **Wednesday, September 20th, from 1:30 pm to 2:15 pm ET.**

For background, the EAC has contracted with Experian, a credit reporting bureau, for the utilization of the bureau's data for purposes of a voter list maintenance pilot project study. This presentation will walk attendees through Orange County, California's process and how they use Experian's tool today, followed by an open discussion with attendees. Experian will be on the call to address any technical questions about the product. **If you are interested in attending this presentation or participating in this pilot study, please complete this survey.**

If you have any questions or concerns, please contact Adam Podowitz-Thomas, Senior Elections Subject Matter Expert, at athomas@eac.gov. Election officials' participation is critical to the success of this study. We appreciate your consideration of this request.

Best,

Kimberly Smith | Senior Election Subject Matter Expert
Alternate Designated Federal Officer (ADFO), Standards Board
U.S. Election Assistance Commission
633 3rd Street NW, Suite 200 | Washington, DC 20001
www.eac.gov

From: Christina Adkins
To: Adam Bitter
Subject: FW: Resignation Notice | Virginia
Date: Thursday, July 13, 2023 3:57:03 PM
Attachments: ERIC Resignation Letter_v1.pdf

From: Hamlin, Shane <shane.hamlin@ericstates.org>
Sent: Thursday, May 11, 2023 4:34 PM
To: Hamlin, Shane <shane.hamlin@ericstates.org>
Cc: Haas, Ericka <ericka.haas@ericstates.org>; Whitt, Sarah <sarah.whitt@ericstates.org>
Subject: Resignation Notice | Virginia

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Sent to ERIC Members & Secondary Points of Contact

Members,

I’m reaching out to inform you that Virginia resigned from ERIC today. Commissioner Beals submitted the attached notice of resignation a short while ago. In compliance with Article II, Sec. 7 of ERIC’s bylaws, Virginia’s resignation takes effect August 10, 2023. Obviously, this is deeply disappointing.

My response to the media will be as follows:

> "ERIC will follow our Bylaws and Membership Agreement regarding any member's request to resign membership. We will continue our work on behalf of our remaining member states in improving the accuracy of America’s voter rolls and increasing access to voter registration for all eligible citizens."
>
> Background: Article II, Section 7 of ERIC's Bylaws specifically addresses resignation. Additionally, I would encourage you to review our "Frequently Asked Questions" for more information.”

Even as we process this news, we have a lot of important work ahead of us. The ERIC team remains focused on supporting your use of ERIC, recruiting new members, and delivering on our mission.

As always, I’m here if you have any questions.

Thank you,

-Shane

Shane Hamlin
Executive Director
ERIC | Electronic Registration Information Center
www.ericstates.org

COMMONWEALTH of VIRGINIA
DEPARTMENT OF ELECTIONS

Susan J. Beals
Commissioner

May 11, 2023

Mr. Shane Hamlin, Executive Director
Electronic Registration Information Center (ERIC)
1201 Connecticut Avenue, NW Suite 600
Washington, DC 20036

Dear Mr. Hamlin:

Virginia was a founding member of ERIC in 2012, joined by seven states committed to appropriately sharing data to improve voter list maintenance. Working with other states to share information that improves the accuracy of voter rolls remains an important goal for Virginia and the Department of Elections. With the recent departures of seven state members, we have reviewed the effectiveness of our continued participation with ERIC.

Based on this careful review, Virginia is terminating its relationship with ERIC for the following reasons:

- Increasing and uncertain costs resulting from the exit of ~20% of ERIC members;
- Incomplete participation of Virginia's bordering states and jurisdictions that compel independent data sharing relationships with non-ERIC members;
- Increasing concerns regarding stewardship, maintenance, privacy, and confidentiality of voter information;
- Controversy surrounding the historical sharing of data with outside organizations leveraged for political purposes;
- Inability to implement meaningful reform to the onerous and inconsistent enforcement of membership requirements in light of recent exits;
- Momentum around the creation of viable alternatives to inter-state data sharing compacts; and
- Virginia's ability to replicate favorable ERIC functionality internally and develop true autonomy for all list maintenance and data sharing practices.

In short, ERIC's mandate has expanded beyond that of its initial intent – to improve the accuracy of voter rolls. We will pursue other information arrangements with our neighboring states and look to other opportunities to partner with states in an apolitical fashion.

Sincerely,

Susan J Beals

Commissioner
Virginia Department of Elections

From: Christina Adkins
To: Elections-Attorneys
Subject: FW: Secretary Nelson in the News 12/14/2023
Date: Thursday, December 14, 2023 9:25:22 AM
Attachments: image001.jpg
image004.png
image003.jpg

From: Alicia Pierce <APierce@sos.texas.gov>
Sent: Thursday, December 14, 2023 9:23 AM
To: Alicia Pierce <APierce@sos.texas.gov>
Subject: Secretary Nelson in the News 12/14/2023

Texas Secretary of State
Morning News Clips
December 14, 2023

Documents show Republican-led states struggling to clean voter rolls after leaving ERIC *VoteBeat* December 13, 2023 (SJN mention)

Spat between local Democrats, Republicans could jeopardize voting for March 2024 primaries *Austin American-Statesman* December 13, 2023

Travis County primary election stalled over disagreements between parties *KVUE* December 13, 2023

Biden considers new border and asylum restrictions as he tries to reach Senate deal for Ukraine aid *Associated Press* December 14, 2023

Documents show Republican-led states struggling to clean voter rolls after leaving ERIC

Jen Fifield
VoteBeat
December 13, 2023
www.votebeat.org /2023/12/13/cleaning-voter-rolls-after-eric-election-security-voter-fraud/

Some Republican-led states are struggling to develop new ways to adequately update their voter rolls after withdrawing from a popular cross-state voter roll cleaning program that came under attack by far-right election activists, according to new documents and internal emails reviewed by Votebeat.

Virginia paid $29,000 in September to regain access to just a sliver of the data they used to obtain via the Electronic Registration Information Center, or ERIC. Alabama and Missouri officials took months to come up with new plans for cleaning voter rolls, landing on plans that are less rigorous than ERIC. And a new system some states are considering to help with voter roll cleanup had its server attacked and temporarily brought down, according to documents obtained by left-leaning watchdog group American Oversight and exclusively shared with Votebeat.

The documents also show that senior advisors to secretaries of state in Missouri and Texas recognized that lies were being spread about ERIC, and tried to stop their states from withdrawing from what they saw as a valuable program. In addition, officials in some states such as Ohio had pushed unsuccessfully for changes to ERIC that could have kept their states from withdrawing.*

“As you know, I really worked as hard as I possibly could to avoid this,” Amanda Grandjean, then the senior advisor to the Ohio secretary of state, wrote in an email to ERIC executive director Shane Hamlin after Ohio withdrew from the program in March.

ERIC is a powerful tool for states to share voter information with other states, allowing them to remove duplicate or dead voters from their rolls. It has been successful mainly because of the sheer volume of the data it collects, which allows it to accurately match voter data on a large scale, and because it has worked through the complications involved in cross-referencing the different data sets and storing and transmitting the data securely.

Before the exodus of members began in early 2022, more than half of U.S. states were participating, and membership was virtually balanced between

Republican- and Democratic-led states.

Clean voter rolls help ensure that eligible voters only cast one ballot, and help counties keep mail voting costs down by eliminating ineligible voters from the rolls. As states leave ERIC, not only do they lose access to the collective's valuable data themselves, their withdrawal means the remaining states have less data with which to clean their own rolls. Michael Morse, a law professor at the University of Pennsylvania who researches voter roll maintenance, said this may not only undermine confidence in elections, but also could cause problems for voters at the polls whose addresses may not be up-to-date after they move, sometimes requiring them to cast a provisional ballot.

"Inaccurate rolls to me are an integrity problem," Morse said. "But, they are also an access problem."

The nine Republican states that have left since 2022 can't replicate this type of system, and are instead taking a piecemeal approach that leaves them contending with a series of challenges, the documents show. For example, a working group involving several states led by Ohio Secretary of State Frank LaRose's office wrestled this spring with the legality and security of data-sharing across state lines, according to emails among state officials.

In the margins of a draft agreement, an official noted they weren't sure whether some states permitted confidential voter data to be shared in the way proposed. "Do other states' laws allow this?" the comment read.

Hamlin, the executive director of ERIC, told Votebeat that its founding states worked for more than two years to build ERIC and "ensure what we do and how we do it complies with state and federal laws," he said in a statement. "We also made sure data privacy and security were built into our processes and practices from the beginning."

So far, instead of a multi-state agreement, states have instead signed individual agreements with other states.

West Virginia, for example, has signed agreements with Ohio, Florida, Virginia, and Tennessee — states likely to have residents moving between them and West Virginia. West Virginia is not attempting to replace ERIC, but primarily trying to identify potentially illegal voting activity across state lines, said Donald Kersey, general counsel for the West Virginia Secretary of State's Office.

Kersey said in an email that it hasn't been complicated.

"It naturally required states to work with each other to find time to meet and review the [memorandums of understanding], but it has been no more complicated than other MOUs our office works on with other entities or state agencies," he wrote. Kersey said the creation of a multi-state agreement wasn't the sole mission of the Ohio-led working group, instead describing it as "part of the discussion," and said the state is also using other sources of data to clean its voter rolls as needed.

States were advised of ERIC's value

The exodus from ERIC began after the far-right website The Gateway Pundit published articles in January 2022 laden with false information about the program: That it had been funded by left-wing financier George Soros and that it was run by virulent partisans who sought to pad voter rolls with liberal voters.

None of that was true, and prior to the onslaught of coverage the program was considered apolitical: A cross-partisan team of officials from member states run the program, and it's funded out of those states' budgets. Along with attempting to match duplicate voters across state lines, the states use the data they receive from ERIC to inform new residents of their state that they are eligible to vote. The dual purpose of the program was what initially attracted both Democratic- and Republican-led states.

When the Gateway Pundit's articles were published, election offices across the country began to get emails from constituents demanding they leave the program. Soon, Republican secretaries of state who had long been proponents of ERIC in the past changed their tune.

Documents show that their top advisors knew that the Gateway Pundit stories were false.

The day after the first article was published on Gateway Pundit's site, ERIC's executive director emailed officials in ERIC member states attempting to debunk it.

"I appreciate you sharing this and will advise the Secretary," Trish Vincent, chief of staff for Missouri Secretary of State Jay Ashcroft, wrote back to Hamlin. "He has gotten some inquiries related to this horrible and misleading article."

But in early March 2023, Ashcroft withdrew Missouri from ERIC, making it the third state to leave the program after Louisiana and Alabama. Florida, West Virginia, Ohio, Iowa, and Virginia left next.

Texas was the most recent. There, too, internal emails from the Secretary of State's Office show that officials there knew that leaving ERIC would be costly and inefficient.

When a chief of staff for a North Texas Republican state lawmaker reached out to Sam Taylor, the assistant secretary of state for communications for Secretary of State Jane Nelson, in January asking him for information about ERIC, Taylor responded with a long email explaining the importance of the program.

Taylor explained that from June to December 2022 alone, ERIC provided the office with information that led to more than 200,000 deceased or duplicate voter records being flagged for county voter registrars to investigate. He also corrected some of the inaccuracies in the Gateway Pundit story, explaining, for example, that ERIC isn't funded by Soros.

Taylor called ERIC an "important election integrity tool," and said without it, counties wouldn't be able to remove certain voters from the rolls, "creating the opportunity for criminals to commit fraud in the name of a deceased person or a person who no longer lives in Texas but is still registered here."

Nonetheless, Texas left ERIC in July.

Taylor, who no longer works for the secretary of state, told Votebeat in a text message Monday that, while ERIC was the best tool states had for cross-state voter roll cleanup, the program became less effective due to the multi-state exodus.

"And whatever new system takes its place will likely face similar scrutiny surrounding transparency, accuracy, and efficacy in helping keep voter rolls clean and up-to-date," he said.

Some states that withdrew cited financial concerns. States spent between $37,000 and $174,000 for annual membership for the most recent fiscal year, depending on their size. But the mailings required by the program cost states as well, and the membership fees are growing as states back out of the program and fewer remain to share the burden.

But any other system may be expensive, too. In a fiscal note obtained by

American Oversight for the legislation that allowed Texas to withdraw from the program, the Texas' Secretary of State's Office estimated that any cost savings the state would see from leaving ERIC, which cost the state $1.5 million every two years, would be "offset by the costs of participating in a different program or in developing a new program."

Christina Adkins, elections director for the Secretary of State's Office, estimated the office would continue to need the $1.5 million every two years for any new system it used to clean voter rolls.

Virginia has already found that getting the data that ERIC provided is costly.

In August, the state paid $3,445 just to get access to the national database that uses Social Security numbers to report deaths, the Limited Access Death Master File, and the next month the state paid $28,960 for a private company to match the files to the Virginia voter roll, one of the many services ERIC previously provided, according to receipts obtained by American Oversight. Membership to ERIC cost Virginia about $40,000 in annual dues for 2019-2020, according to a state document. The dues have since risen, but more recent data wasn't immediately available.

States left ERIC without a replacement plan

The documents show that, in many cases, states that left ERIC didn't have a long-term plan to replace it. At least some also lacked short-term plans for keeping voter rolls up-to-date in the meantime.

In Alabama, for example, Secretary of State Wes Allen ran his 2022 campaign for the office on a platform of removing the state from ERIC. He announced the state's exit from ERIC immediately after taking office in January. Yet two months later, the state's elections director was just starting to figure out how to replace it.

On March 27, Jeff Elrod sent an email to an official with the National Association of State Election Directors asking for contact information for the best person at the U.S. Postal Service to get change-of-address data for voter roll maintenance, something ERIC had provided the state.

Ashcroft withdrew Missouri from ERIC in March, though it appears the state's counties received no formal guidance for months as to how they should now perform voter roll list maintenance without it. On June 7, the elections director of Saint Louis County wrote indicating he'd received the new guide, and asking for an electronic version of it to use for staff training.

Meanwhile, Missouri has joined other states who have departed ERIC in forming a working group to establish a new way to share voter data across state lines. As of this spring, the group was wrestling with both the legal and practical challenges around obtaining and sharing necessary data, and trading tips on possible sources for it while attempting to hammer out a draft template for agreements between states, a June email from Grandjean in Ohio to officials in the group shows.

In addition to questions about whether laws in all the states would allow confidential voter information to be shared and how, working group members also weren't sure how often the states could commit to sharing data with each other. A draft agreement circulating at the time suggested every six months, with a note that said "Discuss." That's much less frequent than ERIC, which requires data sharing at least every 60 days, though it's up to individual states how often they use the available data to update voter rolls.

Grandjean also touched on the cybersecurity questions around how data would be shared.

"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" she wrote, updating the group about a June meeting.

Lawmakers and advocates have suggested some private vendors as replacements for ERIC, but those have also faced security challenges: One private vendor marketing itself as a voter roll cleanup solution across state lines, EagleAI, faced a cyberattack in October, according to the documents.

Columbia County in Georgia recently signed up to use the system. In October, EagleAI CEO John "Rick" Richards Jr. responded to concerns from the county, including a claim that the EagleAI system had been hacked.

On Oct. 4, Richards confirmed via email that "several EagleAI network servers became inoperative," adding that "investigation indicated it was possibly due to an attack on the Windows server software."

In an email to Votebeat, he denied that the event — which he characterized as a "denial of service attack" — put any voter data at risk.

"Denial of service attacks happen all the time, hundreds and even thousands of times a day," Richards wrote. "There was no breech[sic] of the EagleAI software."

Morse said it's not surprising to him that states are laboring to find substitutes for ERIC. ERIC took a long time to create, he said, and reflects a careful design that takes into consideration state and federal laws, as well as secure and accurate sharing of private data.

"The states withdrawing from ERIC cannot just easily stand up a copycat," he said. "I don't expect anyone to stand up a copycat. What I expect is for people to stand up a cheap imitation that will ultimately be worse."

Correction, Dec. 13, 2023: *This story has been updated to correctly reflect the context of the email Amanda Grandjean, then the senior advisor to the Ohio secretary of state, sent to ERIC executive director Shane Hamlin after Ohio withdrew from the program. After this article published, Grandjean told Votebeat the email, which said, "As you know, I really worked as hard as I possibly could to avoid this," referenced her advocacy for changes to ERIC's requirements that might have prevented Ohio's withdrawal. The email did not directly acknowledge that lies were being spread about ERIC.*

Votebeat journalists Natalia Contreras, Carrie Levine, and Carter Walker contributed to this report.

Jen Fifield is a reporter for Votebeat based in Arizona. Contact Jen at jfifield@votebeat.org.

[BACK TO TOP]

Spat between local Democrats, Republicans could jeopardize voting for March 2024 primaries

Austin American-Statesman
December 13, 2023
www.statesman.com /story/news/local/2023/12/13/republicans-democrats-in-stalemate-over-election-contract/71906908007/

A rift between the leaders of the Travis County Democratic and Republican parties could jeopardize where local voters cast a ballot in the March election, which includes a presidential primary.

The local branches of the parties have for years entered into a joint contract for a county-wide election, which allows Travis County residents to vote at any polling place in the county. Negotiations usually don't draw much attention.

This year, however, the Travis County Democratic Party says the local Republican Party has for months caused "chaos and confusion" during negotiations by contemplating a return to precinct-by-precinct voting and the hand-counting of some ballots.

It's a sentiment staunchly contested by the county's Republican party leaders.

Matt Mackowiak, chair of the Travis County Republican Party, told the American-Statesman, "It's a paranoid freak out that has no basis."

"Our draft primary contract included Countywide Voting," Mackowiak said in a statement. "We are going back and forth with edits and hope to complete the primary contract in the next day or so."

Travis County Clerk Dyana Limon-Mercado told the American-Statesman that last week the Travis County Republican Party sent them a contract proposal and that it was unclear if they were proposing a joint or separate primary.

A counter proposal for a joint primary was sent to both parties on Monday, Limon-Mercado said. Both parties have confirmed they received the draft but neither have sent a draft back or an affirmative response as of Wednesday afternoon.

There is no deadline for a contract to be reached, Limon-Mercado said.

A contract was entered for the March 2022 primaries in Travis County by Nov. 30, 2021, Travis County Democratic Party Chair Katie Naranjo said at a news conference Wednesday. The contract was approved by the Travis County Commissioners Court in the first week of December that year.

The first day to apply by mail for a ballot in the March primary is Jan. 1, according to the Texas Secretary of State's website, and the first day of early voting is Feb. 20.

Naranjo said she feels there is still time for the parties to reach an agreement, but if they have to take legal action, the Travis County Democratic Party is prepared to do so.

"Our goal is to be in a contract by the end of this week," Naranjo said.

Similar legislation died in the state House last session

Earlier this year, the Republican-dominated state Senate approved a bill to entirely eliminate the county-wide polling program, which began in earnest with several participating counties in 2008 and has since been utilized by 91 of Texas' 254 counties, according to the Secretary of State's office.

Sen. Bob Hall, R-Edgewood, filed Senate Bill 990 out of a concern that county-wide polling contributes to "vulnerabilities in election security and frustrates chain-of-custody measures."

That argument was harshly contested by Democrats at the time, and again at Wednesday's news conference, as party members accused Republicans of continuing efforts to deny and overturn election results.

"You have no evidence to prove anything that you're saying," Sen. Roland Gutierrez, D-San Antonio, told Hall as the measure advanced to the House along party lines in April.

The Secretary of State's office prior to the start of the legislative session in January made available to lawmakers a report detailing the statewide success of the county-wide voting program, only recommending the program take into consideration the impacts of providing multiple voting locations for smaller, localized elections.

SB 990 ultimately went unheard in the House.

Wednesday, state Sen. Sarah Eckhardt, D-Austin, expressed frustration that the successful voting program has continued to come under partisan scrutiny.

"This is a next iteration of these conspiracy theories that is now bubbled up into procedural chaos," Eckhardt said.

U.S. Congressman Lloyd Doggett, D-Austin, calling the attempted change in voting an overall effort to discourage voting in Travis County, said Texas has been "ground zero" for voter suppression measures as the Legislature has tightened parameters on early and mail in voting along with increasing the penalty for illegal voting to a second degree felony earlier this year.

[BACK TO TOP]

Travis County primary election stalled over disagreements between parties

Laura Sather
(KVUE)
December 13, 2023

AUSTIN, Texas — We are less than three months away from the 2024 primary elections in Texas.

The Democratic and Republican parties in Travis County can't agree on how the March primary should run, and there's concern that it could affect how residents vote.

In Texas, primary elections are organized by the parties, and historically, the parties come to an agreement on the mechanics of primary voting and send that to the clerk's office, which actually runs the primary.

But during a virtual press conference on Wednesday, Travis County Democrats said they should have had a finalized contract last week but Republicans are holding things up. They say Republicans don't want county-wide polling, which allows voters to cast their ballots anywhere in the county, instead of at a specific precinct location, and they say the Republicans want ballots to be hand-counted.

Democrats say a delay in an agreement affects the clerk's office's ability to prepare for March.

"We can get ballots-by-mail out, we can find voting locations, etc. It is Dec. 13 and we are no closer to getting a joint primary negotiated than we were back on Nov. 13," said Chair of the Travis County Democratic Party Katie Naranjo.

Related Articles

- **Election lawsuits could delay implementation of wildly popular constitutional amendments, including tax cuts**
- **'Rogue DA' lawsuit takes aim at Travis County's José Garza**

However, the Travis County Republican Party tells KVUE News it sent a draft contract to the Democrats on Friday that included provisions to have county-wide polling, but it didn't elaborate on the details of that proposal. In a statement, Travis County GOP Chair Matt Mackowiack wrote in part, "Everything we are seeking has been negotiated with Travis County Elections and has been blessed by the Texas Secretary of State's Office."

If the parties don't come to an agreement, there's concern they would have to run the primaries separately, and because Texas has open-primary voting – meaning voters pick which primary, Democrat or

Republican, they want to vote in at the polls – there's really no guidelines for how that might work.

[BACK TO TOP]

Biden considers new border and asylum restrictions as he tries to reach Senate deal for Ukraine aid

STEPHEN GROVES, LISA MASCARO and COLLEEN LONG
Associated Press
December 14, 2023
www.lmtonline.com /news/article/biden-considers-new-border-and-asylum-18552027.php

WASHINGTON (AP) — Top Biden administration officials labored Wednesday to try to reach a last-minute deal for wartime aid for Ukraine by agreeing to Senate Republican demands to bolster U.S.-Mexico border policies, with urgency setting in as Congress prepared to depart Washington with the impasse unresolved.

The White House was racing to lock in a deal in principle with key Senate negotiators, according to two people familiar with the plans who demanded anonymity to discuss them. A core negotiating group, which has included Homeland Security Secretary Alejandro Mayorkas, departed the Capitol Wednesday evening after making progress but without the principles of a deal finalized.

As details of the plan emerged, advocates for immigrants and members of President Joe Biden’s own Democratic Party fretted about the policies under discussion. Some demonstrated at the Capitol, warning of a return to the hardline border and immigration policies of the Trump era.

Congress has little time to reach an agreement on Biden's $110 billion request for Ukraine, Israel and other national security needs that Republicans are holding up to demand changes to border policy. While White House officials and key Senate negotiators appeared to be narrowing in on a list of priorities to tighten the U.S.-Mexico border and remove some recent migrant arrivals already in the U.S., Senate Republicans earlier Wednesday said not enough progress had been made to justify staying in Washington beyond Thursday.

Ukrainian President Volodymyr Zelenskyy visited Washington this week to implore lawmakers for support, but lawmakers were still ready to leave for weeks with one of the U.S.'s key international commitments — helping halt Russian President Vladimir Putin's invasion into Ukraine — seriously in doubt. Also left hanging would be a deal on one of the most unwieldy issues in American politics: immigration and border security.

“The talks are continuing,” said Senate Majority Leader Chuck Schumer as he closed the Senate Wednesday night.

Among the proposals being seriously discussed, according to several people familiar with the private talks, are plans to allow Homeland Security officials to stop migrants from applying for asylum at the U.S. southern border if the number of total crossings exceeds daily capacity of roughly 5,000. Some one-day totals this year have exceeded 10,000.

Also under discussion are proposals to detain people claiming asylum at the border, including families with children, potentially with electronic monitoring systems.

Negotiators are also eyeing ways to allow authorities to quickly remove migrants who have been in the United States for less than two years, even if they are far from the border. But those removals would only extend to people who either have not claimed asylum or were not approved to enter the asylum system, according to one of the people briefed on the negotiations.

The policies resemble ones that President Donald Trump's Republican administration tried to implement to cut border crossings, but many of them were successfully challenged in court. If Congress were to make them law, it would give immigration advocates very little legal ground to challenge the restrictions for those seeking asylum.

Advocates for immigrant warned of a return to anti-immigrant policies and questioned whether they would even address problems at the border.

“I never would have imagined that in a moment where we have a Democratic Senate and a Democratic White House we are coming to the table and proposing some of the most draconian immigration policies that there have ever been,” said Maribel Hernández Rivera, American Civil Liberties Union director of policy and government affairs.

The Senate negotiators had also found some agreement on raising the threshold for people to claim asylum in initial credible fear screenings.

Sen. Chris Murphy of Connecticut, a key Democratic negotiator, said it should be no surprise there are Democrats unhappy about some of the provisions being discussed, which is why they need a balanced agreement.

“I would just say that it’s clear we have to get a lot of Democratic votes and a lot of Republicans in order to pass this and that means making sure that this is a fair agreement,” Murphy said after a long day of talks.

Senate Republicans discussed the White House's proposal at a lunchtime meeting and expressed some optimism that Biden's administration was directly involved in shaping the legislation. But many senators said there was simply not enough time to iron out an agreement.

“Nobody’s written anything up. These are all concepts right now,” said Sen. John Thune, the no. 2 Senate Republican, adding, “The deal has not come together."

But the Senate's most ardent supporters of Ukraine urged congressional leaders to keep lawmakers in Washington until the package is passed. One group of Democratic senators met in Senate Republican Leader Mitch McConnell's office Wednesday afternoon, and Sen. Michael Bennet, a Colorado Democrat who organized the meeting, emerged calling it a “productive" session.

In a separate meeting, Mayorkas met for roughly two hours at the Capitol with a core negotiating group. It was the second day in a row the Cabinet secretary traveled to the Capitol, but issues still remained in striking an agreement.

“Good progress," said Sen. Kyrsten Sinema of Arizona late in the evening.

Even if the Senate stayed in Washington to pass the proposals, House Speaker Mike Johnson of Louisiana, a Republican, would also need to push the legislation through his chamber, where there will likely be opposition from both parties. Hard-line conservatives complain the Senate proposals do not go far enough, while progressive Democrats and Hispanic lawmakers are opposed to cutting off access to asylum.

At a press conference in front of the Capitol, leaders of the Congressional Progressive Caucus and Congressional Hispanic Caucus vowed to oppose the policies under consideration. They also said that Latino lawmakers should have been central to the negotiations.

“(Biden) campaigned on restoring the soul of the nation and holding firm to our democratic values and the principles of our founding fathers. And that includes defending our asylum system and respectful treatment of refugees," said Sen. Alex Padilla, D-Calif.

He called it “unconscionable” for the Democratic president to make concessions on border policy without gaining policies that benefit immigrants.

White House press secretary Karine Jean-Pierre said the administration was “encouraged” by progress in the negotiations and stressed that any final product has to be a “bipartisan compromise.” She declined to address criticism from advocates that the provisions under discussion could be more draconian than that of Biden’s predecessor, Donald Trump.

In the Capitol, the senators who have been negotiating the border package also considered asking to have lawmakers return to Washington next week, hoping that they could use this week's momentum to push through the package.

But their colleagues warned that having the Senate pass the package would be futile unless the House was ready to move quickly.

“It’ll be a piñata out there that people take potshots at for the next couple of weeks,” said Sen. John Cornyn, R-Texas.

Associated Press writers Elliot Spagat, Seung Min Kim and Rebecca Santana contributed to this report.

[BACK TO TOP]

Alicia Phillips Pierce
Assistant Secretary of State for Communications
Office of the Secretary of State
512-463-6116

From: Adam Bitter
To: "Hamlin, Shane"
Cc: Christina Adkins; Kristi Hart; Haas, Ericka; Whitt, Sarah
Subject: RE: Action Requested | TX ERIC Membership Close-out Letter
Date: Wednesday, October 25, 2023 6:11:41 PM

Shane,

Thank you for your response.

It is my understanding that you spoke with Christina and Kristi today about the dues payment. Based on that conversation, I wanted to clarify the part of my letter addressing that issue.

In drafting the letter, I was mistaken about the month through which the State of Texas had already paid dues. Specifically, I understood (incorrectly) that our previous dues payment ran through July 2023 (rather than June 2023). I apologize for any confusion caused by my letter. To clarify, we will remit payment to ERIC for the prorated portion of the State of Texas's annual dues covering the period of **July 1, 2023 through October 19, 2023**.

Upon receipt of an updated invoice from ERIC, we will work with our office's Finance staff to process the payment.

Thank you for your courtesy and professionalism on this matter.

Regards,

Adam

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

From: Hamlin, Shane <shane.hamlin@ericstates.org>
Sent: Wednesday, October 25, 2023 1:26 PM
To: Adam Bitter <ABitter@sos.texas.gov>
Cc: Christina Adkins <CAdkins@sos.texas.gov>; Kristi Hart <KHart@sos.texas.gov>; Haas, Ericka <ericka.haas@ericstates.org>; Whitt, Sarah <sarah.whitt@ericstates.org>
Subject: RE: Action Requested | TX ERIC Membership Close-out Letter

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hello, Adam.

I am in receipt of the letter. Thank you for confirming the hashing application has been disposed of, and I appreciate your office's approach to handling the dues. I'll submit an updated invoice soon.

Please let me know if there is anything else you need from us. Otherwise, I'll close by expressing my appreciation to you, Christina, and Kristi for being excellent partners during the time Texas was a member of ERIC. Thank you.

Sincerely,

Shane Hamlin
Executive Director
ERIC | Electronic Registration Information Center
www.ericstates.org

From: Adam Bitter <ABitter@sos.texas.gov>
Sent: Tuesday, October 24, 2023 1:50 PM
To: Hamlin, Shane <shane.hamlin@ericstates.org>
Cc: Adkins, Christina (TX) <CAdkins@sos.texas.gov>; Hart, Kristi (TX) <khart@sos.texas.gov>; Haas, Ericka <ericka.haas@ericstates.org>; Whitt, Sarah <sarah.whitt@ericstates.org>
Subject: RE: Action Requested | TX ERIC Membership Close-out Letter

Mr. Hamlin,

Please see the attached correspondence from the Office of the Texas Secretary of State in response to your October 9, 2023 letter.

Sincerely,

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

From: Hamlin, Shane <shane.hamlin@ericstates.org>
Sent: Monday, October 9, 2023 4:22:32 PM
To: Christina Adkins <CAdkins@sos.texas.gov>
Cc: Kristi Hart <KHart@sos.texas.gov>; Haas, Ericka <ericka.haas@ericstates.org>; Whitt, Sarah <sarah.whitt@ericstates.org>
Subject: Action Requested | TX ERIC Membership Close-out Letter

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hello, Christina.

Please find attached a membership close-out letter. The purpose of the letter to provide for an orderly withdrawal from ERIC and to clearly communicate any outstanding issues and ongoing obligations ERIC and Texas have. As such, the letter includes several requests for follow-up action.

It was a pleasure to work with you, Kristi, and the other members of your office. Texas made excellent use of ERIC given the statutory constraints your office faced on the list maintenance reports.

As always, please let me know if you have any questions.

Sincerely,

Shane Hamlin
Executive Director
ERIC | Electronic Registration Information Center
www.ericstates.org

From: Adam Bitter
To: "Hamlin, Shane"
Cc: Christina Adkins; Kristi Hart; "ericka.haas@ericstates.org"; "sarah.whitt@ericstates.org"
Subject: RE: Action Requested | TX ERIC Membership Close-out Letter
Date: Tuesday, October 24, 2023 3:49:53 PM
Attachments: Texas SOS Letter to Electronic Registration Information Center (10.24.23).pdf

Mr. Hamlin,

Please see the attached correspondence from the Office of the Texas Secretary of State in response to your October 9, 2023 letter.

Sincerely,

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

From: Hamlin, Shane <shane.hamlin@ericstates.org>
Sent: Monday, October 9, 2023 4:22:32 PM
To: Christina Adkins <CAdkins@sos.texas.gov>
Cc: Kristi Hart <KHart@sos.texas.gov>; Haas, Ericka <ericka.haas@ericstates.org>; Whitt, Sarah <sarah.whitt@ericstates.org>
Subject: Action Requested | TX ERIC Membership Close-out Letter

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hello, Christina.

Please find attached a membership close-out letter. The purpose of the letter to provide for an orderly withdrawal from ERIC and to clearly communicate any outstanding issues and ongoing obligations ERIC and Texas have. As such, the letter includes several requests for follow-up action.

It was a pleasure to work with you, Kristi, and the other members of your office. Texas made excellent use of ERIC given the statutory constraints your office faced on the list maintenance reports.

As always, please let me know if you have any questions.

Sincerely,

Shane Hamlin
Executive Director
ERIC | Electronic Registration Information Center
www.ericstates.org

The State of Texas

Executive Division
Capitol Building, 1E.8
P.O. Box 12697
Austin, Texas 78711-2697

Phone: 512-463-5770
Fax: 512-475-2761
Dial 7-1-1 For Relay Services
www.sos.texas.gov

Jane Nelson
Secretary of State

October 24, 2023

Shane Hamlin
Executive Director
Electronic Registration Information Center, Inc.
1201 Connecticut Ave. NW, Suite 600
Washington, DC 20036

Dear Mr. Hamlin:

The Office of the Texas Secretary of State (the Office) has received your letter dated October 9, 2023, detailing certain matters relating to the State of Texas's resignation from the Electronic Registration Information Center (ERIC). As indicated in your letter, the State's resignation from ERIC was effective on October 19, 2023.

In response to your October 9, 2023 letter, I write to inform you of the following actions:

- The Office has removed, and disposed of, its copies of the ERIC Hashing Application.
- If the Office receives a request for ERIC-related information that is protected from disclosure under federal or state law or regulations, the Office will inform ERIC of that request and comply with state law provisions regarding the withholding of such information from public disclosure.
- The Office has certified its compliance with the ERIC Membership Agreement pertaining to the In-State Updates and Cross-State Movers Reports provided to the State of Texas.
- With respect to the processing of voter participation data, the Office will follow the ERIC Membership Agreement provisions, to the extent that these obligations survive the State's resignation from ERIC, and applicable Texas law.
- By separate transmittal, the Office will remit payment to ERIC for the prorated portion of the State's Fiscal Year 2024 membership dues covering the time period of August 1, 2023 through October 19, 2023. We consider this payment to constitute a full satisfaction of the State's dues obligations under the ERIC Membership Agreement.

Please let me know if you have any questions or need additional information from the Office in connection with the State of Texas's resignation from ERIC.

Sincerely,

Adam Bitter
General Counsel
Office of the Texas Secretary of State

From: Christina Adkins
To: Wendy Underhill
Subject: Re: Any thoughts on an ERIC replacement?
Date: Thursday, June 8, 2023 3:33:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

Hi Wendy,

Thanks for the email! Do you have a couple of minutes where we could chat about this?

Thanks!

Christina

Christina Worrell Adkins
Director of Elections
Office of the Texas Secretary of State
1019 Brazos Street | Rudder Building, 2nd Floor | Austin, Texas 78701
1.800.252.VOTE (8683)
elections@sos.texas.gov | www.sos.texas.gov

For Voter Related Information, please visit:

The information contained in this email is intended to provide advice and assistance in election matters per §31.004 of the Texas Election Code. It is not intended to serve as a legal opinion for any matter. Please review the law yourself, and consult with an attorney when your legal rights are involved.

From: Wendy Underhill <[redacted]
Sent: Thursday, June 8, 2023 1:57:49 PM
To: Christina Adkins <CAdkins@sos.texas.gov>
Subject: Any thoughts on an ERIC replacement?

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hi Christina.

I'm writing a neutral, calm story about the rise and now diminishment of ERIC. If you or Keith are working on a replacement, I'd love to know about it. Is there anything you can offer at this point? Even if I could say "Texas, STATE, STATE and STATE are working on an alternative" that would be good.

I’m hoping something is in writing, saying a replacement is on its way.

Thanks much—even if you just have to say “can’t help this time” it’s good to know you are on the job!

Wendy Underhill
National Conference of State Legislatures
Director, Elections & Redistricting
Office: 303.856.1379 | Cell: 303-802-6673

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.

From: Adam Bitter
To: "Kelly Follis"
Subject: RE: INETMAIL: Election integrity
Date: Wednesday, November 15, 2023 4:55:40 PM

Kelly,

Thanks for your message. I did not receive your email from Tuesday, but I'm not entirely sure why—you used the correct email address. In any event, I got your email from earlier today! I am happy to be the point of contact on the Secretary of State's end for any policy questions involving our office.

You may want to point the constituent in the direction of Senate Bill 1, passed by the 87th Legislature in its Second Called Session. SB 1, as you may know, addressed a host of issues, including vote harvesting, the delivery of mail ballots, and mail ballot verification provisions. Our office released an Election Advisory in November 2021 summarizing the key provisions of SB 1. In addition, we issued an Election Advisory summarizing the major election-related legislation adopted by the 88th Legislature this year, including bills regarding voter list maintenance and signature verification procedures.

Please call me if you would like to discuss this inquiry (or any other SOS-related inquiry) in further detail. I have included my direct contact information below.

Sincerely,

Adam

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

-----Original Message-----
From: Kelly Follis <Kelly.Follis@senate.texas.gov>
Sent: Wednesday, November 15, 2023 10:07 AM
To: Adam Bitter <ABitter@sos.texas.gov>
Subject: RE: INETMAIL: Election integrity

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Good morning!
I'm just making sure you received my email. Thank you!

-----Original Message-----
From: Kelly Follis <Kelly.Follis@senate.texas.gov>
Sent: Tuesday, November 14, 2023 1:16 PM
To: Abitter@sos.Texas.gov
Subject: FW: INETMAIL: Election integrity

Hi Adam,

Joe Esparza indicated that you're the best contact on policy questions. Hopefully, you can help me or direct me to get help on a response to the constituent's email below. I worked for Senator Campbell for 9 years and left to pursue another route but when I recently opened my own business and she offered me a part-time job, I was so happy to come back. All that to say that I wasn't here last session and when you're in the "real world" you don't always follow bills as closely... and even sometimes when my work here isn't connected with a particular issue. Can you please advise about what was done last session? I would appreciate it.. Thank you!

Kelly Donegan Follis
Part-Time District Office Caseworker
(Mon-Wed, 8:30 to 4:30; Thurs, 8:30 to 2:30) Senator Donna Campbell, M.D.
229 Hunters Village, Suite 105
New Braunfels, Texas 78132
830.626.0065

-----Original Message-----
From: [redacted]
Sent: Thursday, November 9, 2023 9:55 AM
To: Donna Campbell <Donna.Campbell@senate.texas.gov>
Subject: INETMAIL: Election integrity

First Name: Randy
Middle Name:
Last Name: Clasen
Suffix:
Title:
Business:

Address line 1: 1722 Sunnybrook
Address line 2:
City: New Braunfels

State: Tx
Zipcode: 78130
Phone: 830-2374368
E-mail: [redacted]

Subject:
Election integrity

Message:
What has the Texas Senate and House done since 2020 to prevent illegal ballot harvesting and stuffing drop boxes, cleaning voter rolls to prevent voter fraud and improve signature verification to stop forgery.

ComputerIP: 108.247.107.213

From: Adam Bitter
To: "Kelly Follis"
Subject: RE: INETMAIL: Election integrity
Date: Thursday, November 16, 2023 9:58:35 AM
Attachments: RE INETMAIL Election integrity.msg

Thanks, Kelly.

I sent you the attached email yesterday afternoon in response to your message from earlier this week. Please let me know if you have any other questions.

Best,

Adam

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

-----Original Message-----
From: Kelly Follis <Kelly.Follis@senate.texas.gov>
Sent: Tuesday, November 14, 2023 1:16 PM
To: Adam Bitter <ABitter@sos.texas.gov>
Subject: FW: INETMAIL: Election integrity

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hi Adam,

Joe Esparza indicated that you're the best contact on policy questions. Hopefully, you can help me or direct me to get help on a response to the constituent's email below. I worked for Senator Campbell for 9 years and left to pursue another route but when I recently opened my own business and she offered me a part-time job, I was so happy to come back. All that to say that I wasn't here last session and when you're in the "real world" you don't always follow bills as closely... and even sometimes when my work here isn't connected with a particular issue. Can you please advise about what was done last session? I would appreciate it.. Thank you!

Kelly Donegan Follis
Part-Time District Office Caseworker
(Mon-Wed, 8:30 to 4:30; Thurs, 8:30 to 2:30) Senator Donna Campbell, M.D.
229 Hunters Village, Suite 105
New Braunfels, Texas 78132
830.626.0065

-----Original Message-----
From: [redacted]

Sent: Thursday, November 9, 2023 9:55 AM
To: Donna Campbell <Donna.Campbell@senate.texas.gov>
Subject: INETMAIL: Election integrity

First Name: Randy
Middle Name:
Last Name: Clasen
Suffix:
Title:
Business:

Address line 1: 1722 Sunnybrook
Address line 2:
City: New Braunfels
State: Tx
Zipcode: 78130
Phone: 830-2374368
E-mail[redacted]

Subject:
Election integrity

Message:
What has the Texas Senate and House done since 2020 to prevent illegal ballot harvesting and stuffing drop boxes, cleaning voter rolls to prevent voter fraud and improve signature verification to stop forgery.

ComputerIP: 108.247.107.213

From: Adam Bitter
To: "Kelly Follis"
Subject: RE: INETMAIL: Election integrity
Date: Wednesday, November 15, 2023 4:55:40 PM

Kelly,

Thanks for your message. I did not receive your email from Tuesday, but I'm not entirely sure why—you used the correct email address. In any event, I got your email from earlier today! I am happy to be the point of contact on the Secretary of State's end for any policy questions involving our office.

You may want to point the constituent in the direction of Senate Bill 1, passed by the 87th Legislature in its Second Called Session. SB 1, as you may know, addressed a host of issues, including vote harvesting, the delivery of mail ballots, and mail ballot verification provisions. Our office released an Election Advisory in November 2021 summarizing the key provisions of SB 1. In addition, we issued an Election Advisory summarizing the major election-related legislation adopted by the 88th Legislature this year, including bills regarding voter list maintenance and signature verification procedures.

Please call me if you would like to discuss this inquiry (or any other SOS-related inquiry) in further detail. I have included my direct contact information below.

Sincerely,

Adam

Adam Bitter
General Counsel
Office of the Texas Secretary of State
(512) 475-2813
abitter@sos.texas.gov

-----Original Message-----
From: Kelly Follis <Kelly.Follis@senate.texas.gov>
Sent: Wednesday, November 15, 2023 10:07 AM
To: Adam Bitter <ABitter@sos.texas.gov>
Subject: RE: INETMAIL: Election integrity

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Good morning!
I'm just making sure you received my email. Thank you!

-----Original Message-----
From: Kelly Follis <Kelly.Follis@senate.texas.gov>
Sent: Tuesday, November 14, 2023 1:16 PM
To: Abitter@sos.Texas.gov
Subject: FW: INETMAIL: Election integrity

Hi Adam,

Joe Esparza indicated that you're the best contact on policy questions. Hopefully, you can help me or direct me to get help on a response to the constituent's email below. I worked for Senator Campbell for 9 years and left to pursue another route but when I recently opened my own business and she offered me a part-time job, I was so happy to come back. All that to say that I wasn't here last session and when you're in the "real world" you don't always follow bills as closely... and even sometimes when my work here isn't connected with a particular issue. Can you please advise about what was done last session? I would appreciate it.. Thank you!

Kelly Donegan Follis
Part-Time District Office Caseworker
(Mon-Wed, 8:30 to 4:30; Thurs, 8:30 to 2:30) Senator Donna Campbell, M.D.
229 Hunters Village, Suite 105
New Braunfels, Texas 78132
830.626.0065

-----Original Message-----
From: [redacted]
Sent: Thursday, November 9, 2023 9:55 AM
To: Donna Campbell <Donna.Campbell@senate.texas.gov>
Subject: INETMAIL: Election integrity

First Name: Randy
Middle Name:
Last Name: Clasen
Suffix:
Title:
Business:

Address line 1: 1722 Sunnybrook
Address line 2:
City: New Braunfels

State: Tx
Zipcode: 78130
Phone: 830-2374368
E-mail: [redacted]

Subject:
Election integrity

Message:
What has the Texas Senate and House done since 2020 to prevent illegal ballot harvesting and stuffing drop boxes, cleaning voter rolls to prevent voter fraud and improve signature verification to stop forgery.

ComputerIP: 108.247.107.213

From: Christina Adkins
To: Christy Wilson
Subject: Re: Invite
Date: Wednesday, February 7, 2024 12:43:16 PM
Attachments: image001.png

Christy, Thank you so much for the invitation! I already have a dinner commitment tonight so I won't be able to make it. And sadly, Kristi is staying back in Texas for this trip to get things moving along while I'm in DC.

I'll look for you all to say hello if you will be around the conference tomorrow.

Christina

From: Christy Wilson <cwilson@gocivix.com>
Sent: Tuesday, February 6, 2024 5:06:19 PM
To: Christina Adkins <CAdkins@sos.texas.gov>
Subject: Invite

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Hi Christina,

Karen (my colleague in the East) and I are organizing a dinner with a select group of clients to discuss states needs/ideas for the Voter Registration list maintenance and State cross checking. We're excited about the interest from several states and would greatly value your perspective on how the state imagines securely sharing data, with our role being to provide the essential infrastructure for these verifications.

I have reached out to representatives from Iowa, Louisiana, and yourself, while Karen has invited West Virginia. This will be a casual gathering, offering an opportunity for Leslie Eagle, our Director of Product Management, to engage closely with our stakeholders and address the challenges we aim to tackle.

The dinner is set at Bobby Van's @ 7PM on Wednesday Feb. 7th, conveniently located near the hotel. Please let me know if you'll be able to join us. Also, if you're traveling with anyone, feel free to bring them along – we're happy to welcome more guests! (I thought Kristi told me she was hanging back in Texas).

Best,

Christy Wilson
Strategic Account Director

Cell 405.818.4701
400 International Parkway, Suite 400
Heathrow, FL 32746-5037

GoCivix.com

From: Christina Adkins
To: "Lindsey Forson"
Subject: RE: NASS Cybersecurity Committee: Webinar Follow-up
Date: Wednesday, December 13, 2023 2:08:38 PM
Attachments: Election Security Toolkit Templates.zip
image001.png

Hi Lindsey,

I saw that you were looking for state examples of COOP/Incident Response Plans. I've attached the Election Security Toolkit that we customized specifically for elections in Texas. We worked with a vendor on this back in 2019. This is a template that we provide to our election officials so that they have something to work off of in developing their own local plans. We also offer regional workshops to help them complete the plans. I'm happy to share this resources with other states that may find them helpful.

Additionally, we put out this Election Security Best Practices Guide that may be helpful as well.

Let me know if there's anything you need from us in Texas.

Thanks,

Christina Worrell Adkins
Director of Elections
Office of the Texas Secretary of State
1019 Brazos Street | Rudder Building, 2nd Floor | Austin, Texas 78701
512-463-9859 (direct) | 1.800.252.VOTE (8683)
elections@sos.texas.gov | www.sos.texas.gov
For Voter Related Information, please visit:

The information contained in this email is intended to provide advice and assistance in election matters per §31.004 of the Texas Election Code. It is not intended to serve as a legal opinion for any matter. Please review the law yourself, and consult with an attorney when your legal rights are involved.

From: Lindsey Forson [redacted]
Sent: Wednesday, December 13, 2023 9:14 AM
Subject: NASS Cybersecurity Committee: Webinar Follow-up

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear NASS Cybersecurity Committee and relevant staff,

This email is to follow up on our recent NASS webinar: Essential Cybersecurity for Secretary of State Offices. Attached are the presentation slides and an overview of potentially relevant federal and state entities. Please do not distribute these materials outside your office.

The webinar presenters included cybersecurity leaders from several state offices. They shared their perspectives on key cybersecurity topics and how their offices approach some cybersecurity issues. It is important to note: We understand that each state is different. NASS is not making any specific recommendations. However, we hope the webinar provided some useful insight for your team.

Thank you again to the webinar sponsors, VOTEC and Democracy Live, and to the presenters from West Virginia, New York, Ohio, and Minnesota! Let me know if you have any questions or would like any additional information. We got one request for COOP/incident response plan examples or templates. We are working to identify some updated state examples. In the meantime, here is a resource from CISA that may be helpful.

Happy holidays to all of you!

Lindsey

Lindsey Forson
Deputy Executive Director
National Association of Secretaries of State (NASS)
444 N. Capitol Street NW, Suite 401
Washington, DC 20001
202-624-3524 (office)
904-687-9387 (cell)
www.nass.org

HOW TO USE THIS CONTINUITY OF OPERATIONS PLAN TEMPLATE

This document is the **Continuity of Operations Plan (COOP)**. It details how Election Authority employees, early voting and election day workers, and vendors protect election information from theft, loss, and manipulation. You, the Election Authority should revise this plan to make it relevant to your staff, early voting and election day workers, and vendors, your office environment and voting facilities, your resources, and your election processes.

In the Election Security Best Practices Guide provided in the Texas Election Security Toolkit, the Texas Secretary of State (SOS) prescribes the creation of an Election Written Information Security Program (WISP). An Election WISP is a set of five documents establishing policies that protect elections from cyber threats as well as plans that keep elections running in the event of a cyberattack or disruption.

Documents that comprise the Written Information Security Policy (WISP):

1. Election Information Security Policy
2. Security Incident Response Plan
3. Continuity of Operations Plan
4. Election System Security Plan
5. Vendor Risk Management Policy

IMPORTANT THINGS TO KNOW ABOUT THIS DOCUMENT

- This document provides a **Plan** that defines the guidance your agency will follow and the actions that must be taken if election operations are disrupted by a cyberattack or other disaster event. The plan created is expected to be authorized by your County and used for many years, even as your staff and County continue to change.
- When completed, this document will serve as **Your Plan** that you must adopt and adapt to the needs of **Your County**. SOS provides this template as a starting place, but you are expected to review and make changes, as appropriate for your County. **County Election Authority Leadership is ultimately responsible for the security of its election.**
  - Many of the actions and considerations defined in this plan will apply to most Election Authorities. Depending on the needs of your organization, your plan may have additional guidelines, or it may not have as many.
  - Some of the operation continuity instructions in this plan template may not apply to you because of variations in facilities, organizational structure, and other factors, but your Election Authority must follow all of the prescribed continuity of operations instructions that are relevant to your organization.
- This plan template must be reviewed and updated before being adopted by your county.
  - Some continuity of operation plan instructions and worksheets will require you to fill in the details specific to your organization. These areas are pre-filled with suggestions or examples marked with underlined and italicized text.
  - You are encouraged to add your own specific plan instructions if you need to clarify or prescribe continuity of operation actions for purposes that are unique to your environment.

- The Appendices consist-of example logs and forms to use when assigning staff continuity of operations responsibilities and logging or tracking processes as defined in the plan. These are worksheets that are not considered part of the Election Information Security Plan because they are continuously updated in the course of daily tasks.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR PLAN

1. Read through the entire plan template without making any changes, so you understand its full scope.
2. Read through the plan template again, this time marking each instruction as belonging to one of the following categories:
    - **Yes**

      Applies to you and no revisions are needed
    - **Yes +**

      Applies to you, but needs to be refined with simple known revisions that make it relevant
    - **Maybe**

      Applies to you, but needs additional information that is not yet known or needs decisions that can only be made by someone else or a group of people
    - **No**

      Does not apply to you because the instruction references a process or resource that is not needed by your organization
3. Start working on adapting the plan to your specific criteria by making the needed revisions to the “Yes +” category.
4. Delete the instructions that fall into the “No” category.
5. Gather the information needed for the “Maybe” category and obtain the needed decisions.

- Delete an instruction or plan element if a decision deems it no longer applicable to you and puts it in the "No" category.
- Add decisions to your plan that fall into the "Yes" category.

6. Replace the underlined, italicized suggestions with your own details.
7. Make copies of the logs and forms in the Appendices and use these copies to keep track of your processes in the event of a cyberattack or other disaster event.

After you tailor this document to your election organization, it will become your Continuity of Operations Plan (COOP) and a part of your Election WISP. Follow the storage and document management processes for this document and for the rest of the Election WISP as defined in your Election Information Security Policy.

HOW TO USE THIS DOCUMENT

Once this document becomes your official Continuity of Operations Plan (COOP), it will be a living document that should be reviewed regularly and adapted to your organization as circumstances and processes change.

To use this document:

- Ensure that the information and resources needed to execute the COOP (as defined in the Appendices) have been created and assembled and are consistently updated so that they are current and easily accessible during an attack or disaster.
- Make sure all staff members know about the COOP, what it contains and where to find it. Review the COOP during staff onboarding and as part of the security awareness training required in the Election Information Security Policy.

- Ensure that staff members who have assigned roles and responsibilities in the COOP know the actions they need to take during an attack or disaster.
- Review the COOP annually or more frequently following the instructions in the Document Management section of this document.
- During a cyberattack or other disaster, immediately locate the COOP, distribute copies to staff members, and emphasize the importance of following the COOP procedures throughout the duration of the incident.
- After the incident is over, meet with staff members to review what worked well, the aspects of the COOP that can be improved, and where additional clarity is required. Update the COOP with the revisions.

ASSISTANCE FROM TEXAS SOS ELECTION SECURITY TRAINERS

If you have questions or need help customizing this Continuity of Operations Plan to your election organization and processes, contact the Texas Secretary of State Office at electionsecurity@sos.texas.gov to request assistance from an election security trainer.

DOCUMENT MANAGEMENT

The Continuity of Operations Plan (COOP) must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements, new cyber threats emerge, or organizational changes require plan updates between yearly reviews.

Maintain a record of all plan reviews in the Plan Review Log to validate that the COOP is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

PLAN REVIEW LOG

PLAN ADOPTED DATE <Date>						
Drafted By	<Name, Title>	Signature	<Signature>	<Date>		
Approved By	<Name, Title>	Signature	<Signature>	<Date>		
REVIEW AND REVISION LOG						
REVIEW SCHEDULE	General Election Years: December after elections			Legislative Session Years: July after SOS Law Conference		
Review Date	If Revised, Revision Date	Revision Description (Or Specify “No	Drafted By: Name, Title	Signature, Date	Approved By: Name, Title	Signature, Date

		Revisions” If None Made)				

[ELECTION AUTHORITY NAME]

CONTINUITY OF OPERATIONS PLAN FOR ELECTIONS

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *[Election Authority Name]* that is classified as Confidential. Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.

The following types of confidential information may be contained in this Policy:

System names and purposes

Security device configuration information

Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is *[Election Authority Name]* Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *[Election Authority Name].*

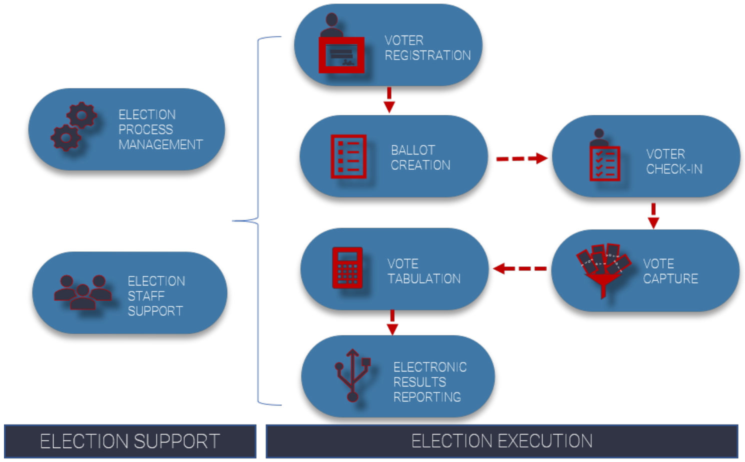
Contents

INTRODUCTION

PURPOSE

The purpose of the Continuity of Operations Plan (COOP) is to define a step-by-step process for keeping election functions operational during disruptions such as those caused by cyberattacks or other disaster events. The critical nature of elections makes it imperative that the Election Authority maintains a current version of this plan and that the plan is reviewed and updated on a regular basis. As a crucial element of the Election Written Information Security Program (WISP), the COOP directs staff on how to ensure an election can be held without delay or disruption even under negative circumstances.

The COOP is aligned to eight main election function areas including staff support, election management, voter registration, ballot creation, voter check-in, vote casting and capture, vote tabulation, and results reporting. This alignment ensures that plans for continued operation are in place to accommodate the potential impact a cyberattack or other disaster event could have on each function.



ASSUMPTIONS

The Continuity of Operations Plan (COOP) is based on several assumptions related to the nature of the incident and the Election Authority's security awareness and preparedness.

The plan assumes that a cyberattack or disaster event has resulted in one or more of the following circumstances:

- Internet or phone access is no longer available
- Network is down and not accessible
- Election voting equipment is not operational
- ePollbooks are not operational
- Tabulation machines are not operational
- Critical staff members are not able to perform their duties
- Essential computers are compromised and can't be used
- Critical applications are compromised and can't be used
- Election administration main office is not usable
- One or more polling locations is not usable

The COOP also assumes that:

- The election team has complied with the requirements of the Election Information Security Policy, particularly:
    - Maintaining a frequently updated encrypted external hard drive with backups of critical data [*located in a safety deposit box at a bank or other offsite location*]

    - Maintaining an inventory of all essential technology and equipment
    - Maintaining a current diagram of the network
    - Adhering to the Election Data Classification System in the Election Information Security Policy to ensure that critical information is protected and backed up
  - A Cybersecurity Incident Response Plan (IRP) is in place and the team is familiar with it. The IRP defines:
    - What constitutes a cyberattack incident and when to activate the Security Incident Response Plan
    - The members of the incident response team and their roles during an incident
    - An escalation path for notifying the response team and the appropriate resources
    - A communication plan that is aligned to the data handling criteria specified in the Election Data Classification System
- The following resources and information needed to support the COOP have been identified or created and assembled in a series of appendices listed here:
  - Election Continuity of Operations Contact List (Appendix A)
  - Early Voting and Election Day Worker Contact List (Appendix B)
  - Responsibility Succession Plan (Appendix C) and each next-in-line designee has been assigned login credentials for critical systems or applications
  - Job Responsibilities and Task Guide (Appendix D) for individuals with responsibility for critical business functions
  - Alternate Utilities and Facilities Plan (Appendix E)
  - Relocation Checklist (Appendix F)

CONTINUITY OF OPERATIONS FOR ESSENTIAL ELECTION FUNCTIONS

ELECTION STAFF SUPPORT

This section references the underlying processes and technologies that enable the Election Authority's business operations.

- □ The Election Administrator is responsible for ensuring that election staff have the resources needed for continuity of business operations.
- □ If the [*Election Administrator*] is not available, refer to the Responsibility Succession Plan (Appendix C) and contact the next-in-line designee.
  - ○ The *[Election Administrator]* is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role.
- □ Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - ○ These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents are also maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*]. Refer to Table 1: Election Staff Support Alternative Technology and Data Plan for information about how to access the backups of the Job Responsibilities and Tasks Guide, if needed.
- □ If regular communication capabilities such as office phone or email are lost, communication capabilities must be maintained via call and text using cell phones.

- ○ Refer to the Election Continuity of Operations Contact List (Appendix A) to find mobile phone contact information.

□ If any office systems related to managing elections are compromised or damaged, the [*Election Administrator*] is responsible for implementing alternate technology and data as outlined in Table 1: Election Staff Support Alternative Technology and Data Plan with support from the [*IT Director or IT Vendor*].

- ○ These systems include:
  - ▪ Staff computers
  - ▪ Office productivity software
  - ▪ Network connectivity
  - ▪ Internet access
  - ▪ Email functionality
  - ▪ Phone systems

□ If data has been lost or access to data is unavailable, retrieve the backups of the data needed to support the election team's functions.

- ○ [*Two copies*] of electronic, encrypted hard drive with data backups are regularly updated [*once per month*] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
- ○ When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
  - ▪ This data includes:
    - • Business operation plans and budgets

    - Human Resources records
    - Documented employee job functions with access credentials
    - Contact lists
    - Election Written Information Security Program (WISP), which includes:
        - Election Information Security Policy
        - Security Incident Response Plan
        - Election System Security Plan
        - Election Vendor Risk Management Policy
        - This Continuity of Operations Plan

- □ If the Election Office is not usable or power is not available for extended time periods, [*the ABC High School library has been designated as an alternate election team office site*].
    - Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.
    - If relocation is needed, refer to the Relocation Checklist (Appendix F), coordinate the collection and transportation of needed items, and set up at the alternate site.
- □ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing business operations technology lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 1: Election Staff Support Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Computer Needed for Essential Functions	Prepared replacement computer 1	Locked 2nd floor storage closet	Key to closet	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Computer Needed for Essential Functions	Prepared replacement computer 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Internet Access	Mobile Hotspot Device 1	Locked 2nd floor storage closet	Key to closet and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Voter Registrar	123-456-7890

Internet Access	Mobile Hotspot Device 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Email Functionality	Cell Phone Numbers for Calls and Texts	Refer to Election Continuity of Operations Contact List	N/A				
Data Needed for Essential Business Operations	Data Backup on Encrypted Hard Drive 1	Locked 2nd floor storage closet	Key to closet	Election Administrator	123-456-7890	Voter Registrar	123-456-7890

Data Needed for Essential Business Operations	Data Backup Encrypted Hard Drive 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Primary Staff Member(s) Responsible for Staff Support Functions	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890

ELECTION MANAGEMENT

This section references the underlying technologies and processes that enable the Election Authority's election operations.

- □ If election systems are compromised or damaged, the [*Election Administrator*] is responsible for implementing alternate election systems with support from the [*Voter Registrar and Office Manager*] and election equipment vendors.
  - These systems and resources include:
    - Access to Secretary of State resources
    - Voting machines
    - Tabulation machines
    - ePollbooks
    - Website and social media channels
  - Refer to Table 2: Election Management Alternative Technology and Data Plan for information on resources available for use if any of these systems is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) and contact the next-in-line designee if the *[Election Administrator] or other personnel with critical election management duties* is not available.
  - The [*Election Administrator*] and other personnel with critical election management duties are responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role.
- □ Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.

- These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].
- Refer to Table 2: Election Management Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guides if needed.

□ Refer to the Early Voting and Election Day Worker Contact List (Appendix B) for contact information and engage the Early Voting and Election Day Worker Coordinator who will serve as the single point of contact for communicating emergency and/or alternative procedure instructions and for receiving information from early voting and election day workers in the event of a cyberattack or disaster event.

□ If regular communication capabilities such as office phone or email are lost, staff members and early voting and election day workers must use cell phones to maintain communication capabilities via call and text. Refer to the Election Continuity of Operations Contact List (Appendix A) and Early Voting and Election Day Worker Contact List (Appendix B) to find mobile phone contact information.

□ If data needed to support election management is lost, or access to the data is unavailable, retrieve the backups of the needed data.

- This data includes:
    - Voter registration data
    - Candidate information
    - Polling location details

        - ▪ Early Voting and Election Day Worker Contact List (Appendix B)
        - ▪ Ballot designs and source files
    - ○ [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [once per month] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
    - ○ When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.
- □ If the polling locations are not usable or power is not available for extended time periods, move polling operations to the facility near the polling location designated as the backup location in the Alternate Utilities and Facilities Plan (Appendix E). Visible signs must be posted at the original polling location directing voters to the alternate location.
- □ Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on alternate facilities for each polling location and for details on when and how to relocate if necessary.
- □ If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.
- □ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing business operations technology lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 2: Election Management Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Computer Needed for Essential Election Management Functions	Prepared replacement computer 1	Locked 2nd floor storage closet	Key to closet	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Computer Needed for Essential Election Management Functions	Prepared replacement computer 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890

Internet Access	Mobile Hotspot Device 1	Locked 2nd floor storage closet	Key to closet and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Internet Access	Mobile Hotspot Device 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Email Functionality	Use Cell Phones or Calls and Texts	Refer to the Election Continuity of Operations Contact List	N/A				

Data Needed for Essential Election Management	Data Backup on Encrypted Hard Drive 1	Locked 2nd floor storage closet	Key to closet	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Data Needed for Essential Election Management	Data Backup Encrypted Hard Drive 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890
Primary Staff Member(s) Responsible for Election Management	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Voter Registrar	123-456-7890

VOTER REGISTRATION

This section references the underlying technologies and processes that enable the County Election Department to register voters, validate identities, and confirm voter eligibility before, during and after an election.

- □ The [*Voter Registrar*] is responsible for voter registration functions, ensuring records are accurately entered into the electronic systems, securely retaining paper copies, and programming ePollbooks with support from the [*Election Administrator*] and election system vendors.
  - ○ These systems and resources include:
    - ▪ Access to the State Voter Registration System
    - ▪ ePollbooks
  - ○ Refer to Table 3: Voter Registration Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the [*Voter Registrar*] is not available.
  - ○ The [*Voter Registrar*] is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The *[Voter Registrar]* must also ensure that the next-in-line designee understands the voter registration process and records retention requirements.
- □ Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - ○ These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and

one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].

- Refer to Table 3: Voter Registration Alternative Technology and Data Plan for information on how to access the backups of election technology and supporting systems, if needed.
- If data needed to support voter registration is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
  - Voter registration data including back up electronic or paper lists of registered voters
  - Instructions for registering to vote
  - Processes for various registration and renewal methods.
  - Documented voter registration-related job functions
- [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [daily] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

Table 3: Voter Registration Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

Computer Needed for Voter Registration Functions	Prepared replacement computer 1	Locked 2nd floor storage closet	Key to closet	Voter Registrar	123-456-7890	Election Administrator	123-456-7890
Computer Needed for Voter Register Functions	Prepared replacement computer 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Voter Registrar	123-456-7890	Election Administrator	123-456-7890
Internet Access to Voter Registration System	Mobile Hotspot Device 1	Locked 2nd floor storage closet	Key to closet and access credentials for Mobile Hotspot	Voter Registrar	123-456-7890	Election Administrator	123-456-7890
Internet Access to Voter Registration System	Mobile Hotspot Device 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval and access credentials	Voter Registrar	123-456-7890	Election Administrator	123-456-7890

			for Mobile Hotspot				
Primary Staff Member(s) Responsible for Voter Registration	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Voter Registrar	123-456-7890	Election Administrator	123-456-7890
Voter Registration Data	Voter Registration Data Backup on Encrypted Hard Drive 1	Locked 2nd floor storage closet	Key to closet	Voter Registrar	123-456-7890	Election Administrator	123-456-7890
Voter Registration Data	Voter Registration Data Backup	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Voter Registrar	123-456-7890	Election Administrator	123-456-7890

	Encrypted Hard Drive 2						
Electronic Access to Voter Registration Data	Paper Voter Registration Records	Locked filing Cabinet in locked 2nd floor storage closet	Key to Cabinet and Key to Closet	Voter Registrar	123-456-7890	Election Administrator	123-456-7890

BALLOT CREATION AND DISTRIBUTION

This section references the underlying technologies and processes that enable the County Election Department to create ballots and program voting machines.

- □ The [*Election Coordinator*] is responsible for overseeing ballot creation and ensuring that ballots are accurately programmed into voting machines with support from the [*Voter Registrar*] and election system vendors.
  - ○ These systems and resources include:
    - ▪ Design software
    - ▪ Voting machines
  - ○ Refer to Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the [*Election Coordinator*] is not available.
  - ○ The [*Election Coordinator*] is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The [*Election Coordinator*] must also ensure that the next-in-line designee understands the ballot creation and distribution process.
- □ Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - ○ These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and

one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].

- ○ Refer to Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guide (Appendix D), if needed.
- ○ If data needed to support ballot creation is lost or access to the data is unavailable, retrieve the backups of the needed data. This data includes:
  - ▪ Ballot design templates
  - ▪ The final version of approved candidate and proposition information to be included on ballot
  - ▪ Instructions on programming voting machines with ballot information
  - ▪ Documented ballot creation and voting machine programming job functions
- ○ [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [once per month] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
- ○ When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

- During elections, the final ballots must be stored electronically offsite in a location that only the [*Election Coordinator*] can quickly access and send to print should voting machines become inoperable and paper ballots become necessary. Refer to the Election Continuity of Operations Contact List (Appendix A) for the contact information of the printer standing by for immediate response if this situation arises.

- □ During elections, the [*Voting Machine Vendor*] is on call to assist with ballot issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).
- □ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing voting machines lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 4: Ballot Creation and Distribution Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Computer Needed to Create Ballots	Prepared replacement computer 1	Locked 2nd floor storage closet	Key to closet	Election Coordinator	123-456-7890	Assistant Election Coordinator	123-456-7890
Computer Needed to Create Ballots	Prepared replacement computer 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890

Access to Candidate Information	Candidate Data Backup on Encrypted Hard Drive 1	Locked 2nd floor storage closet	Key to closet	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890
Access to Candidate Information	Candidate Data Backup Encrypted Hard Drive 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890
Access to Master Ballot Design Template Electronic File	Master Ballot Backup on Encrypted Hard Drive 1	Locked 2nd floor storage closet	Key to closet	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890
Access to Master Ballot Design Template Electronic File	Master Ballot Backup Encrypted Hard Drive 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890

Primary Staff Member(s) Responsible for Creating Ballots	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Election Coordinator	123-456-7890	Voter Registrar	123-456-7890

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION

This section references the underlying technologies and processes that enable the County Election Department to generate and distribute ePollbooks and facilitate the voter check-in process.

- □ The [*Election Administrator or Designee*] is responsible for overseeing ePollbook programming or the creation of the paper Official List of Registered Voters (OLRV) with support from the [*Voter Registrar*] and election system vendors.
  - These systems and resources may include:
    - ePollbooks
    - Access to voter registration system
    - Internet access through a Virtual Private Network (VPN)
  - Refer to Table 5: ePollbook/Voter Check-In and Qualification Alternate Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the [Elections Administrator or Designee] is not available.
  - The [Elections Administrator] is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The [Elections Administrator] should also ensure that the next-in-line designee understands ePollbook programming or the creation of the paper Official List of Registered Voters (OLRV) process.
- □ Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.

- These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].
- Refer to Table 5: ePollbook/Voter Check-In Alternative Technology and Data Plan for information on how to access the backups of job process documentation, if needed.
- If data needed to support ePollbook creation is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
    - Voter registration data
    - ePollbook and paper OLRV design templates
    - Instructions on programming ePollbooks with voter check-in/qualification information
    - Documented ePollbook and voter check-in/qualification job functions
- [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [*once per month or daily during the voting period*] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
- When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

□ **Paper OLRV Counties –** During elections, the final Official List of Registered Voters (OLRV) should be stored in an electronic file both in house and offsite in the event that voter qualification must take place over the phone.

- □ **ePollbook Counties –** During elections, the final voter registration ePollbook electronic file and a printed copy of the paper OLRV are stored both in house and at an offsite location so that the [*Elections Administrator or Designee*] can quickly access and send to print should ePollbooks become inoperable and backup paper OLRVs become necessary. Contact the pre-designated printing company capable of rapid bulk printing that is standing by for immediate response if this situation arises. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information of the printing company.
- □ During elections, the [*ePollbook Vendor*] is on call to assist with ballot issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).
- □ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing ePollbooks lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 5: ePollbook/Voter Check-In and Qualification Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE
Internet Access to Voter	Mobile Hotspot Device 1	Locked 2nd floor storage closet	Key to closet and access credentials	Voter Registrar	123-456-7890	Office Manager	123-456-7890

Registration System			for Mobile Hotspot				
Internet Access to Voter Registration System	Mobile Hotspot Device 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval and access credentials for Mobile Hotspot	Voter Registrar	123-456-7890	Office Manager	123-456-7890
One ePollbook	Spare ePollbook 1	Locked 2nd floor storage closet	Key to closet	Voter Registrar	123-456-7890	Office Manager	123-456-7890
One ePollbook	Spare ePollbook 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Voter Registrar	123-456-7890	Office Manager	123-456-7890
All ePollbooks	Contact Equipment	N/A	Contact Info: Rep Name	Voter Registrar	123-456-7890	Office Manager	123-456-7890

	Vendor to Initiate Previously Negotiated Emergency Equipment Replacement Plan		Phone # Email				
All ePollbooks	Printed ePollbooks	Create		Voter Registrar	123-456-7890	Office Manager	123-456-7890
Primary Staff Member(s) Responsible for ePollbook Creation and Voter Check-In	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Voter Registrar	123-456-7890	Office Manager	123-456-7890

VOTE CASTING AND CAPTURE

This section references the underlying technologies and processes that enable the County Election Department to facilitate vote casting and capture.

- □ The [*Election Coordinator*] is responsible for regularly testing voting machines' functionality to ensure that they are operating correctly and for arranging transport to and from polling locations with support from the [*Election Administrator*] and election system vendors.
    - ○ These systems and resources include:
        - ▪ Voting machines
            - Acceptance testing
            - Preparation prior to election
            - Hardware testing
            - Logic and accuracy testing
            - Post-election maintenance
    - ○ Refer to Table 6: Vote Casting and Capture Alternative Technology and Data Plan for information about technology and data sources that should be used if any of these resources is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) to find who must be contacted if the [*Election Coordinator*] is not available.
    - ○ The [*Election Coordinator*] is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The [*Election*

Coordinator] should also ensure that the next-in-line designee understands the vote casting and capture process and knows how to troubleshoot common voting machine issues.

- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].
  - Refer to Table 6: Vote Casting and Capture Alternative Technology and Data Plan for information on how to access the backups of Job Responsibilities and Tasks Guide, if needed.
  - If data needed to support vote casting and capture is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
    - Inventory of voting machines
    - Instructions on testing voting machines
    - Instructions on operating voting machines
    - Documented voting machine operations and maintenance job functions
  - Retrieval of data may involve returning equipment to the manufacturer or vendor
    - Acceptance testing after equipment is repaired by vendor

  - [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [once per month] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
  - When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

□ During elections, the [*Voting Machine Vendor*] is on call to assist with voting machine issues or recovery processes. Refer to the Responsibility Succession Plan (Appendix C) and Election Continuity of Operations Contact List (Appendix A).

□ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing voting machines lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 6: Vote Casting and Capture Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

One Voting Machine	Spare Voting Machine	Locked 2nd floor storage closet	Key to closet	Election Coordinator	123-456-7890	Election Administrator	123-456-7890
Many or All Voting Machines	Contact Equipment Vendor to Initiate Previously Negotiated Emergency Equipment Replacement Plan	N/A	Contact Info: Rep Name Phone # Email	Election Coordinator	123-456-7890	Election Administrator	123-456-7890

Primary Staff Member(s) Responsible for Testing and Managing Voting Machines	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in Locked 2nd floor storage closet, or on backup hard drive	Key to closet, key to safety deposit box, box number and approval	Election Coordinator	123-456-7890	Election Administrator	123-456-7890

VOTE TABULATION

This section references the underlying technologies and processes that enable the County Election Department to count votes and determine results.

- The [*Central Counting Station Manager*] is responsible for testing the tabulation computer prior to the election and collecting and tabulating votes into final counts in a secure manner with the required two-person validation support from the [*Tabulation Supervisor*].
    - The required include:
        - Tabulation computer
        - Testing materials
    - Refer to Table 7: Vote Tabulation Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the [*Central Counting Station Manager*] and [*Tabulation Supervisor*] are not available.
    - The [*Central Counting Station Manager*] and [*Tabulation Supervisor*] are responsible for ensuring that the next-in-line designees have the required login credentials and the appropriate level of access permissions needed if the next-in-line designees must take over the tabulation roles. The [*Central Counting Station Manager*] and [*Tabulation Supervisor*] should also ensure that the next-in-line designees understand how to test the tabulation computer before an election as well as the process of tabulating votes and the importance of two-person validation. Individuals selected for this job must be able to accurately perform the duties at the end of a long day.

- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
  - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].
  - Refer to Table 7: Vote Tabulation Alternative Technology and Data Plan for information on how to access the backups of the Job Responsibilities and Tasks Guide (Appendix D), if needed.
  - If data needed to support vote tabulation is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
    - Instructions on testing the tabulation computer
    - Instructions on operating the tabulation computer
    - Instructions on repairing or replacing the tabulation computer
    - Procedures for replacing the tabulation computer in the middle of an election
    - Documented vote tabulation job functions
  - [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [*once per month*] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].
  - When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

- □ An arrangement for repairing or replacing the tabulation computer in the middle of an election has been made with the vendor. During elections, the procedures and instructions for repairing or replacing the tabulation computer are printed and posted near the tabulation computer with the contact number for the vendor. The [*Voting System Vendor*] is on call to assist with recovery processes during elections. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.
- □ Vote tabulation should take place in a pre-designated secured counting room. If the counting room is not usable, or if power is not available, [*the ABC High School principal's office has been designated as an alternate counting room*]. Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.
- □ If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.
- □ The [*Election Administrator*] must contact the insurance company that holds the cyber incident and disaster insurance policy to arrange coverage for the cost of replacing tabulation computers lost to damaging events, if applicable. Refer to the Election Continuity of Operations Contact List (Appendix A) for contact information.

Table 7: Vote Tabulation Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

Tabulation Computer	Backup Tabulation Computer, if available	Locked 2nd floor storage closet	Key to closet	Central Counting Station Manager	123-456-7890	Tabulation Supervisor	123-456-7890
Backup Tabulation Computer, if available	Contact Equipment Vendor to Initiate Previously Negotiated Emergency Equipment Replacement Plan	N/A	Contact Info: Rep Name Phone # Email	Central Counting Station Manager	123-456-7890	Tabulation Supervisor	123-456-7890
Primary Staff Member(s) Responsible for Testing Tabulation	Next-in-Line Designee Follows Documented Job Duties	Documents in Election WISP binder in locked 2nd floor storage closet, or on	Key to closet, key to safety deposit box, box number and approval	Central Counting Station Manager	123-456-7890	Tabulation Supervisor	123-456-7890

Computer and Tabulating Votes		backup hard drive					

ELECTION NIGHT REPORTING

This section references the underlying technologies and processes that enable the County Election Department to securely report accurate results.

- □ The [*Election Administrator*] is responsible for testing the election night reporting procedures prior to every election and for reporting the official election results.
  - ○ The required systems include:
    - ▪ Secure computer
    - ▪ Internet connectivity to access the Secretary of State's Election Night Reporting Interface
    - ▪ Device, cell phone, or application needed for multi-factor authentication
    - ▪ Batteries and chargers to keep computer, phone, and devices charged
    - ▪ County election website
  - ○ Refer to Table 8: Election Night Reporting Alternative Technology and Data Plan for information on technology and data sources that should be used if any of these resources is compromised.
- □ Refer to the Responsibility Succession Plan (Appendix C) to find who should be contacted if the [*Election Administrator*] is not available.
  - ○ The [*Election Administrator*] is responsible for ensuring that the next-in-line designee has the required login credentials and the appropriate level of access permissions needed if the next-in-line designee must take over the role. The [*Election Administrator*] should also ensure that the next-in-line designee understands the election night reporting process and the sensitivities involved.

- Next-in-line designees must refer to the Job Responsibilities and Tasks Guide (Appendix D) and follow the instructions for assuming the responsibilities of the role.
    - These documents are stored with the Election Written Information Security Program (WISP) in an electronic format backed up to two encrypted external hard drives, one stored securely onsite in the [*locked 2nd floor storage closet*] and one stored offsite in [*a safety deposit box at First Dollar Bank*]. The documents will also be maintained in a paper format in the Election WISP binder stored in the [*locked 2nd floor storage closet*].
    - Refer to Table 8: Election Night Reporting Alternative Technology and Data Plan for information on how to access the backups of the Job Responsibilities and Tasks Guide (Appendix D), if needed.
    - If data needed to support election night reporting is lost, or if access to the data is unavailable, retrieve the backups of the needed data. This data includes:
        - Instructions on accessing the Secretary of State's election night reporting interface including the two-step multi-factor authentication login
        - Instructions on posting results to the county's official website and using social media only to direct the public to the county's official website for results
        - Documented election night reporting and publishing job functions
    - [*Two copies*] of the encrypted external hard drives with data backups are regularly updated [once per month] and stored offline. One is stored [*onsite in the locked 2nd floor storage closet and the other offsite in a safety deposit box at First Dollar Bank*].

      When using the backed-up data, continue to follow data management policies according to the Election Data Classification System in the Election Information Security Policy.

- □ Prior to the election, the [*Election Administrator*] will have added the Secretary of State Hotline Number as a contact on their cell phone and programmed with speed dial. If the alternative technologies in Table 8: Election Night Reporting Alternative Technology and Data Plan fail, the [*Election Administrator*] will call in the election results to the Secretary of State's hotline.
- □ Election night reporting is pre-designated to take place in the [*Election Administrator's office*], which ensures reliable internet access and access to the multi-factor authentication methods required to report to the Secretary of State. If the [*Election Administrator's office*] is not usable, or if power is not available, [*the ABC High School principal's office has been designated as an alternate counting room*]. Refer to the Alternate Utilities and Facilities Plan (Appendix E) for details on when and how to relocate if necessary.
- □ If relocation is needed, refer to the Relocation Checklist (Appendix F) to make sure all needed items are transported and set up at the alternate site.

Table 8: Election Night Reporting Alternative Technology and Data Plan

WHAT IS COMPROMISED	ALTERNATIVE	LOCATION	HOW TO ACCESS IT	ROLE WITH ACCESS OR RESPONSIBILITY TO TAKE ACTION			
				PRIMARY	DESK PHONE	NEXT-IN-LINE	DESK PHONE

Computer Needed to Report Results	Prepared replacement computer 1	Locked 2nd floor storage closet	Key to closet	Election Administrator	123-456-7890	Election Coordinator	123-456-7890
Computer Needed to Report Results	Prepared replacement computer 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval	Election Administrator	123-456-7890	Election Coordinator	123-456-7890
Internet Access to SOS and County Election Website	Mobile Hotspot Device 1	Locked 2nd floor storage closet	Key to closet and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Election Coordinator	123-456-7890

Internet Access to SOS and County Election Website	Mobile Hotspot Device 2	Safety Deposit Box at First Dollar Bank	Key to safety deposit box, box number and approval and access credentials for Mobile Hotspot	Election Administrator	123-456-7890	Election Coordinator	123-456-7890
All Alternate Computers and Internet Access	Cell Phone to Call the SOS Office and Provide Results	SOS Number Programmed in Designated Reporter's Cell Phone with Access to MFA	N/A				

APPENDIX A: ELECTION CONTINUITY OF OPERATIONS CONTACT LIST

This list must be maintained and updated regularly [*once per month*] with contact information for all staff members, agencies, and entities involved in ensuring the continuity of operations during a cyberattack or disaster event. This list is not the same as the Incident Response List in the Security Incident Response Plan although some contacts may be on both lists. This list is for distribution to a wider group of staff members with responsibilities for keeping operations running during an attack or disaster.

An electronic copy of the contact list must be available to staff and included in the data backup [*every month*]. Additionally, [*a paper copy must be kept in a file in the Election Administrator's office*]. **Managers and employees with Incident Response and Continuity of Operations duties must keep these names and numbers programmed into their phone contact lists for quick reference.**

NAME	TITLE	PHONE	ALTERNATE/CELL PHONE	EMAIL	STREET ADDRESS	DEPARTMENT/ VENDOR/ AGENCY
Jane Smith	Election Administrator	123-456-7890	123-456-7890	jane@county.gov	County Courthouse 1 Main St. Anywhere, USA 11111	County Election Department
Joe Miller	Sales Engineer	123-456-7890	123-456-7890	jmiller@acme.com	1 Industrial Blvd. Anywhere USA 11111	Acme Voting Machines Inc.

Mary Parker	Sheriff	123-456-7890	123-456-7890	Mary@county.gov	County Courthouse 1 Main St. Anywhere, USA 11111	Police Dept.
Pete Stevens	Emergency Management Coordinator	123-456-7890	123-456-7890	pete@county.gov	County Courthouse 1 Main St. Anywhere, USA 11111	Emergency Response
Hal Martinez	Account Representative	123-456-7890	123-456-7890	Hal@insurance.com	1 Business Way, Anywhere USA 11111	Cyber Insurance Carrier
Kasey Felder	Account Representative	123-456-7890	123-456-7890	kasey@printerhero.com	2 Business Ave, Anywhere USA 11111	Printer on notice during elections that can handle bulk printing

APPENDIX B: EARLY VOTING AND ELECTION DAY WORKER CONTACT LIST

In addition to the Election Continuity of Operations Contact List (Appendix A) maintained year-round, an Early Voting and Election Day Worker Contact List (Appendix B) must be maintained and updated regularly [*weekly during the two months preceding an election*] with contact information for all early voting and election day workers and personnel that interact with and manage early voting and election day workers through the course of managing and facilitating elections.

- During elections, designate an early voting and election day worker coordinator as a single point of contact for communicating emergency and/or alternative procedure instructions and for receiving information from early voting and election day workers in the event of a cyberattack or disaster event.

A copy of the list must be retained and included in the data backup [*monthly during the two months preceding the election*]. Additionally, [*a paper copy will be maintained in the election emergency preparedness binder*].

NAME	EARLY VOTING AND ELECTION DAY WORKER TITLE	PHONE	ALTERNATE/CELL PHONE	EMAIL	LOCATION
Bob Burns	Early Voting and Election Day Worker Coordinator	123-456-7890	123-456-7890	bob@gmail.com	Main Office
Wendy Wills	Sales Engineer	123-456-7890	123-456-7890	wwills@yahoo.com	Polling Location 543

APPENDIX C: RESPONSIBILITY SUCCESSION PLAN

If a team member or critical vendor contact is unable to perform the assigned role, that person's duties must become the responsibility of an assigned individual specified in the following table. It is the responsibility of each primary individual to document the functions of the job, including how to access locked and secured assets and to train the next-in-line designee on what will be required to take over the role. Additionally, access credentials and administrative permissions must be established for the next-in-line individual.

ROLE	DUTIES	PRIMARY	MOBILE #	NEXT-IN-LINE DESIGNEE	MOBILE #	NEXT-IN-LINE HAS DOCUMENTED JOB FUNCTIONS?	NEXT-IN-LINE HAS NEEDED CREDENTIALS AND PERMISSIONS?
Election Administrator	• Maintain Election Operations During Incident • Determine the Appropriate Continuity Plan Elements to Enact • Determine the Needed Replacement/Backup Equipment, Technology and Supplies to Deploy • Immediately Restore Critical Data from	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	Yes

	Backup Hard Drive if Needed - Notify Secretary of State’s Office - Follow Incident Response Plan Procedures if Incident Is Severe Enough - Notify Law Enforcement, State DIR and Any Other Entities Necessary						
Voter Registrar	- Maintain Access to Voter Registration Data - Protect Data from Compromise - Create Ballots - Program Ballots into Voting Machines	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	Yes
IT Director	- Determine Severity of the Incident - Restore Full Operability as Quickly as Possible - Advise Affected Staff on How to Stop Further Damage - Advise Staff on Which Systems Are Operational and Which Are Unavailable During Mitigation	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	Yes

	• Mitigate Cyber Incident • Assemble the Technical IR Team Members						
Early Voting and Election Day Worker Coordinator	• Inform Early Voting and Election Day Workers of Emergency or Temporary Operations and Procedures • Notify EA of Issues at Polling Locations	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	No
Office Manager	• Assist EA in Maintaining Operations • Program Data into ePollbooks • Assemble the Needed Backup Technology, Equipment, Information and Supplies	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	Yes
Communications Director	• Inform the Media According to the Data Classification System • Serve as Point of Contact for All Information Flowing in and Out of Election Department	Jane Smith	123-456-7890	John Doe	123-456-7890	Yes	Yes

	• Keep EA Informed of Developments and Communication Activities • Facilitate Communication Between Departments Involved						
Voting System Vendor	• Maintain Voting System Operability	Jane Smith	123-456-7890	John Doe	123-456-7890	N/A	N/A
ePollbook Vendor	• Maintain ePollbook Operability	Jane Smith	123-456-7890	John Doe	123-456-7890	N/A	N/A
Cyber Incident and Election Equipment Insurance Provider, if applicable	• Cover Cost of Damage Caused by Cyber Incident and Election Equipment Replacement	Jane Smith	123-456-7890	John Doe	123-456-7890	N/A	N/A

APPENDIX D: JOB RESPONSIBILITIES AND TASKS GUIDE

All personnel responsible for essential business functions must make a copy of this table and use it to document their job processes in a detailed, step-by-step format that is easy for a next-in-line designee to follow if the responsible person is unavailable to perform the duties and the next-in-line designee must assume the role.

JOB RESPONSIBILITIES AND TASKS GUIDE			
Title: Election Coordinator			
Critical Responsibilities	Step-by-Step Task Instructions	Resources Needed	Resource Location
Arrange Voting Machine Transport to Polling Locations	1 Create maps from courthouse to polling locations 2 Contact secure courier and arrange pick-up and delivery date 3 On delivery day, maintain accurate Chain of Custody record	• Polling location addresses • Courier contract • Chain of Custody form	• File cabinet in Dan’s office in folder marked “Polling Sites” • File cabinet in Dan’s office in folder marked “Vendors” • Election WISP binder in locked 2nd floor storage closet

APPENDIX E: ALTERNATE UTILITIES AND FACILITIES PLAN

If a building is rendered unusable due to a power failure or disaster event, the following table describes the planned steps for a temporary solution or where to relocate to in order to keep operations running.

ISSUE	SOLUTION	CONTACT		WHO IS RESPONSIBLE FOR TAKING ACTION			
			ESTIMATED COSTS	PRIMARY	MOBILE #	NEXT-IN-LINE DESIGNEE	MOBILE #
Short Term Electricity Outage at Election Main Office	Rent Generators from ABC Hardware as Per Negotiated Plan Requiring Them to Keep Three Generators on Reserve During Election Week	ABC Hardware Contact Info: Rep Name Phone # Email		Jane Smith	123-456-7890	John Doe	123-456-7890
Longer Duration Electricity Outage at Election Main Office	Set up Temporarily at the ABC High School library as Per Negotiated Arrangement with	ABCHS Principal Contact Info: Name Phone # Email		Jane Smith	123-456-7890	John Doe	123-456-7890

	the School Board and Principal.						
Electricity Outage at Polling Location	Rent Generators from ABC Hardware as Per Negotiated Plan Requiring Them to Keep Three Generators on Reserve During Election Week	ABC Hardware Contact Info: Rep Name Phone # Email		Jane Smith	123-456-7890	John Doe	123-456-7890
Election Main Office Is Unusable	Set up Temporarily at the ABC High School library as Per Negotiated Arrangement with the School Board and Principal.	ABCHS Principal Contact Info: Name Phone # Email		Jane Smith	123-456-7890	John Doe	123-456-7890
Counting Room and Election Main Office is	Set up Temporarily at the ABC High School principal office as	ABCHS Principal Contact Info: Name		Jane Smith	123-456-7890	John Doe	123-456-7890

Unusable for Tabulation	Per Negotiated Arrangement with the School Board and Principal.	Phone # Email					
Election Administrator Office and Election Main Office is Unusable for Election Results Reporting	Set up Temporarily at the ABC High School principal office as Per Negotiated Arrangement with the School Board and Principal.	ABCHS Principal Contact Info: Name Phone # Email		Jane Smith	123-456-7890	John Doe	123-456-7890
Polling Location 1 is Unusable	Move to ABC Warehouse on the Next Block	Polling Location Lead		Jane Smith	123-456-7890	John Doe	123-456-7890
Polling Location 2 is Unusable	Move to ABC Gym Across the Street	Polling Location Lead		Jane Smith	123-456-7890	John Doe	123-456-7890

APPENDIX F: RELOCATION CHECKLIST

ITEM	LOCATION	WHO IS RESPONSIBLE
Computers	Individual Desks	Each Staff Member Is Responsible for His or Her Computer
Written Information Security Program Binder	Locked 2nd floor closet	Election Administrator
Backup Hard Drive	Locked 2nd floor closet	Election Administrator
Mobile Hotspot Device	Locked 2nd floor closet	Election Administrator
Spare Tabulation Computer	Locked 2nd floor closet	Election Administrator
Main Tabulation Computer	Office 112	Office Manager
Batteries and Chargers	Office 1B	Office Manager
Extension Cords	Office 1B	Office Manager
Encrypted USB Keys	Office 1B	Office Manager

HOW TO USE THIS POLICY TEMPLATE

This document is the **Election Information Security Policy** that details how Election Authority employees, volunteers and vendors protect election information from theft, loss and manipulation. Election Authorities should revise this policy to make it relevant to your staff, volunteers and vendors, your office environment and voting facilities, your resources and your election processes.

In the Election Security Best Practices Guide provided in the Texas Election Security Toolkit, the Texas Secretary of State (SOS) prescribes the creation of an Election Written Information Security Program (WISP). An Election WISP is a set of five documents establishing policies that protect elections from cyber threats as well as plans that keep elections running in the event of a cyberattack or disruption.

1. Election Information Security Policy
2. Election Incident Response Plan
3. Election Continuity of Operations Plan
4. Election System Security
5. Election Vendor Risk Management Policy

A technical Election Information Security Policy Guide is available upon request from electionsecurity@sos.texas.gov. It details how policies in this document align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a widely accepted standard for security.

IMPORTANT THINGS TO KNOW ABOUT THIS DOCUMENT

- This document provides **Policies** that define the guidelines you will follow as you create plans and practices to secure your election. The policies created are expected to be authorized by your county and used for many years, even as your staff and county continues to change.
- When completed, this is document defines **Your Policies** that you must adopt and adapt to the needs of **Your County**. SOS provides this template as a starting place, but you are expected to review and change, as appropriate for your County. **County Election Authority Leadership are ultimately responsible for the security of your election.**
    - Many of the 21 information security policies defined in this policy will apply to most Election Authorities. You may wind up with a different total number of policies, depending on the needs of your organization.
    - Some of the security practices may not apply to you because of variations in facilities, organization structure and other factors, but Election Authorities should implement all of the security practices that are relevant to your organization.
- This provided template must be reviewed and updated before use.
    - Some security practices will require that you fill in the details specific to your organization. These areas are pre-filled with suggestions or examples marked with underlined and italicized text.
    - You are encouraged to add your own specific security practices if you need to clarify or prescribe security for purposes that are unique to your environment.

- The Appendices consist of example logs and forms to use when assigning staff security responsibilities and logging or tracking processes as defined in the policy. These are worksheets that are not considered part of the Election Information Security Policy because they are continuously updated in the course of daily tasks.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR POLICY

1. Read the policy in its entirety first without making any changes for the purpose of understanding the full scope of the policy.
2. Read the policy again and mark each practice as belonging to one of the following categories:
    - **Yes**
      Applies to you and no revisions are needed
    - **Yes +**
      Applies to you, but needs to be refined with simple known revisions that make it more relevant
    - **Maybe**
      Applies to you, but needs additional information that is not yet known or decisions that can only be made by someone else or a group of people
    - **No**
      Does not apply to you because the practice references a process or resource that is not needed by your organization
3. Start working on adapting the policy to your specific criteria by making the needed revisions to the "Yes +" category.
4. Delete the practices that fall into the "No" category.
5. Gather the information needed for the "Maybe" category and obtain the needed decisions.
    - Delete a practice if a decision deems it no longer applicable to you and puts it in the "No" category.
    - Add decisions to your policy that fall into the "Yes" category.
6. Replace the underlined, italicized suggestions with your own details.
7. Make copies of the logs and forms in the Appendix and use the copies to keep track of your day-to-day processes.

After you tailor the document to your election organization, this document is your Election Information Security Policy and a part of your Election WISP. Follow the storage and document management processes for this document and the rest of the Election WISP as defined in this policy.

ASSISTANCE FROM TEXAS SOS ELECTION SECURITY TRAINERS

If you have questions or need help customizing this Election Information Security Policy to your election organization and processes, contact the Texas Secretary of State Office at electionsecurity@sos.texas.gov to request assistance from an election security trainer.

DOCUMENT MANAGEMENT

The Election Information Security Policy must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements or new cyber threats require policy changes between yearly reviews.

Maintain a record of all policy reviews in the Policy Review Log to validate that the Election Information Security Policy is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

POLICY REVIEW LOG

<table>
<tr><td colspan="7">POLICY ADOPTED DATE <Date&gt;</td></tr>
<tr><td colspan="2">Drafted By</td><td colspan="2">&lt;Name, Title&gt;</td><td>Signature</td><td>&lt;Signature&gt;</td><td>&lt;Date&gt;</td></tr>
<tr><td colspan="2">Approved By</td><td colspan="2">&lt;Name, Title&gt;</td><td>Signature</td><td>&lt;Signature&gt;</td><td>&lt;Date&gt;</td></tr>
<tr><td colspan="7">REVIEW AND REVISION LOG</td></tr>
<tr><td colspan="2">REVIEW SCHEDULE</td><td colspan="3">• General Election Years: December after elections</td><td colspan="2">• Legislative Session Years:July after SoS Law Conf</td></tr>
<tr><td>Review Date</td><td>If Revised, Revision Date</td><td>Revision Description (Or Specify “No Revisions” If None Made)</td><td>Drafted By: Name, Title</td><td>Signature, Date</td><td>Approved By: Name, Title</td><td>Signature, Date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

ELECTION AUTHORITY NAME

ELECTION INFORMATION SECURITY POLICY

Contents

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *Election Authority Name* that is classified as Confidential. Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.

The following types of confidential information may be contained in this Policy:

System names and purposes

Security device configuration information

Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is *Election Authority Name* Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *Election Authority Name*.

INTRODUCTION

The *Election Authority Name* Election Information Security Policy defines the security policies required to protect technology, data and operations from the cyberattacks threatening elections. The Policy incorporates the Security Best Practices developed by the Texas Secretary of State (SOS) in compliance with HB1421 (2019) legislation adopted to protect elections from cyber threats. It is also aligned to the five core objectives outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF):

- IDENTIFY (ID)
- PROTECT (PR)
- DETECT (DE)
- RESPOND (RS)
- RECOVER (RC)

This Policy is a living document that is regularly updated as *Election Authority Name* builds stronger defenses, addresses new cyber threats, and adapts to changing technology.

POLICY SCOPE

- The Policy applies to any individual and entity participating in any capacity in the management, operation and support of *Election Authority Name* elections, election systems and technology.
- The Policy applies to technology, data management, election processes and staff behaviors.
- The Policy encompasses all systems, devices and computers that transmit, receive, and store information used by and for *Election Authority Name.*
- The Policy meets applicable federal, state and local laws in addition to *Election Authority Name* policies, regulations and contractual obligations.

SECTION 1: IDENTIFY

POLICY 1: GOVERNANCE

Election Authority Name follows the guidelines and practices defined in our Election Written Information Security Program (WISP), of which this policy document is a part.

POLICY STANDARDS

- Maintain an updated and authorized Election Written Information Security Program (WISP) which is a set of documents comprised of these five documents:
    1. Election Information Security Policy
    2. Cybersecurity Incident Response Plan
    3. Continuity of Operations Plan
    4. Election System Security Plan
    5. Vendor Risk Management Policy
- Current and future versions of Election WISP policies and plans are approved by (*Specify who has approval authority such as the Election Administrator or County Commissioner.)* to ensure that staff has the pre-authorization needed to prevent a cyberattack or take immediate action during an incident. Election WISP policies and plans can be approved as a set of all five documents or they can be approved individually, especially if major revisions are made to only one document.
- The digital version of the Election WISP is stored in (*Specify a secure location on your network that only election staff can access. Include a file name, folder name and the exact location.),* and access is limited to election staff only.
- An up-to-date printed copy of the Election WISP is stored in a binder located (*Designate a physical location where access can be restricted to authorized employees only such as a locked storage closet.)* If the digital version is inaccessible during a cyberattack, the printed version should be retrieved by election staff only.
- All policies and plans in the Election WISP are reviewed and updated according to the following schedule:
    - During general election years, in December after an election to incorporate lessons learned or changes to the election process
    - During legislative session years, in July after the Secretary of State Election Law Conference to incorporate any new laws
- The Policies in the Election WISP apply to any individual and entity participating in any capacity in the management, operation and support of elections, election systems and technology.

- Security responsibilities by employee role are assigned and approved by *(Specify the role with authority to assign and approve security responsibilities. This could be the Election Administrator.)* They are documented and tracked using the Security Roles and Responsibilities Chart.

POLICY 2: BUSINESS ENVIRONMENT

Election Authority Name clearly states our elections mission and identifies the operations critical to accomplishing it. Security decisions are focused on protecting the operations that support the mission.

MISSION STATEMENT
(Record your mission statement here. Example: To provide our community with safe, secure and accurate elections with the highest level of integrity and transparency.
CRITICAL OPERATIONS
Voter Registration
Providing Voter and Candidate Information to the Community
Ballot Creation and Loading Ballots to Voting Machines
Ballot by Mail Operations
Poll Worker Coordination and Communication
Transportation of Voting Machines and Ballots to and from Polling Locations
Voter Check-In and Verifying Identity and Eligibility
Secure Transmission of Voter Data to Polling Locations and from Central Servers in Real Time
Unofficial Results Tabulation
Deliver Results to the Public
Canvass of Official Results
Secure Storage of Voting Devices, Election Records, and Electronic Media During the Preservation Period

POLICY STANDARDS

- Our mission statement and the operations critical to accomplishing our mission are clearly defined in written form. NOTE: This mission statement is not a security statement; it is a statement that defines our overall purpose so that we can make security decisions that best protect our ability to fulfill this mission.
- The mission statement and critical operations list must be reviewed as part of the annual Election WISP review required in Policy 1 to make sure they are current and accurately reflect the operations with the most potential to disrupt elections if they are compromised by a cyberattack.

- When writing or updating plans such as the Continuity of Operations Plan, the Incident Response Plan and the Election System Security Plan, the mission statement and critical operations list must be referenced to make sure the plans address the protection and recovery of operations that support our mission.
- The mission statement and critical operations list are included in the Information Security Awareness Training required in Policy 10.

POLICY 3: SECURITY RISK ASSESSMENT AND MANAGEMENT STRATEGY

The election team stays informed of cybercrime targeting elections and takes steps to manage those risks.

POLICY STANDARDS

- A subscription to the Department of Homeland Security Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) information sharing services must be continuously maintained.
- The processes outlined in our Threat and Risk Monitoring Log worksheet (sample in the Appendix B) must be followed to stay informed of, record and act on MS-ISAC, EI-ISAC and media reports of cyber threats that specifically pose a potential threat to the organization.
- The risk of significant threats to the critical operations that support the mission statement and the overall election process must be assessed as soon as we receive reports of new threats.

POLICY 4: SUPPLY CHAIN RISK MANAGEMENT

Third-party vendors must comply with the Vendor Risk Management Policy included in the Election WISP.

POLICY STANDARDS

- The Vendor Risk Management Policy must be reviewed updated if needed at least yearly as part of the Policy 1 Election WISP annual review requirement.
- Vendor risk should be evaluated annually by checking with vendors to see if any significant changes to their networks, technologies or business processes have recently occurred and by staying informed of cyber threat risks that could affect our vendors via the ISAC information sharing subscription.
- All contracts, supply agreements and service level agreements will specify that the vendor agrees to comply with the Vendor Risk Management Policy.
- A staff escort is required for third-party vendors visiting our facilities, and vendors who regularly work in our facilities are required to have identification badges without unlocking or door access capabilities..
- Vendor risk will be evaluated annually as part of the Election WISP review described in Policy 1.

POLICY 5: ASSET MANAGEMENT

An inventory of devices, systems, equipment, software and data ranked by criticality is created and maintained by the Elections Department and/or IT.

POLICY STANDARDS

- An accurate inventory of election systems *(Specify the election systems and devices you are responsible for managing such as voting machines and pollbooks)* must be created and updated annually following the Inventory
- Create and annually update an inventory of all general technology assets including:
  - Election Authority-issued Employee Devices (laptops, desktops, tablets)
  - Servers and Storage Devices
  - Software Including Cloud Software
  - Network Equipment (firewalls, routers, switches, monitoring systems)
- The IT team's inventory must uniquely identify each technology asset by including:
  - Model
  - Serial Number
  - Location
- The inventory ranks the criticality of each asset using the Technology Asset Criticality Classification System in Table 1 that reflects the importance of each technology asset to mission-critical operations.
- The inventory includes chain of custody information for critical assets such as:
  - Person who issued the item
  - Person using the item
  - Person receiving the item when it's returned
- The inventory must include a change management log documenting significant updates, patches and changes made to critical assets.
- Each asset is managed according to security guidelines defined in the Technology Asset Criticality Classification System in Table 2 below.
- Removable media devices should be included in the inventory, and their use and management must comply with the Removable Media Policy. An example of a Removable Policy is in the Appendix D.
- A diagram depicting the network design and data flow of critical operations must be created and stored with the asset inventory.

TABLE 1: TECHNOLOGY ASSET CRITICALITY CLASSIFICATION SYSTEM

CRITICALITY LEVEL	ASSETS INCLUDED, BUT NOT LIMITED TO	SECURITY GUIDELINES
1	Servers storing voter and candidate information Election systems ePollbooks Website Server and/or Hosting Account Voter Registration System Account Encrypted Backup Hard Drive	• Physical Assets ○ Assets must be stored in a locked location ○ A two-person verification record in an access log is required for entry to area ○ Access is limited to authorized personnel only ○ Written approval must be obtained before access to the area is granted ○ Physical assets in offsite locations such as IT vendor facilities must be stored in a locked area with restricted and controlled access • Software Assets ○ Access is limited to authorized personnel only with strict limitations on who receives administrator privileges ○ Written approval is required before access credentials or administrator privileges will be granted ○ Unique usernames must be used ○ Credential sharing is strictly prohibited ○ Strong passwords are required ○ Multifactor authentication is required where possible ○ On premise assets must be contained within the election network firewall

		○ Remote and Internet access is restricted ○ Continuous monitoring for suspicious activity is required ○ Data must be backed up using encryption ○ Chain of custody record is required
2	Employee desktops and laptops Mobile devices Productivity Software Social media accounts	• Physical Assets ○ Protect physical access to hardware assets by keeping them in a locked area when not in use ○ Assignment log is required ○ Limit area access to personnel or escorted visitors only • Software Assets ○ Approval process not required, but access credentials should be assigned to personnel only ○ Assign unique usernames and prohibit credential sharing ○ Require strong passwords ○ Require multifactor authentication where possible ○ Keep the asset located behind election-specific firewall in the network ○ Remote access via a Virtual Private Network permissible ○ Monitor for suspicious activity ○ Backup data using encryption
3	Printers Copy Machines Fax machines	• Locked area not required, but advised • Require strong passwords if needed • Multifactor authentication not required

		• Monitor for suspicious activity

SECTION 2: PROTECT

POLICY 6: DATA SECURITY AND INFORMATION PROTECTION

The Election Data Classification System must accurately include all election data types and correctly categorize the data according to how stringently it should be protected. Election-related data must be inventoried, labeled and secured consistent with the Election Data Classification System (Table 2).

POLICY STANDARDS

- An accurate inventory of all major data sets that are managed, stored and used to support elections must be created and annually updated using the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log in the Appendix C.
- The data inventory must include classification levels of election data according to the Election Data Classification System in Table 2 below.
- Data will be consistently backed up to *(Specify backup location or method such as an encrypted hard drive)* that is not connected to the Internet or the election network and that is stored offsite *(Specify a safe offsite location such as a safety box at a nearby bank.)*
- Encryption must be used to protect Confidential, Sensitive and Internal Use election data as it is sent between systems and offices and while it is stored.
- Confidential, Sensitive and Internal Use data must be permanently deleted from decommissioned computers, devices, servers, hard drives and removable media before they are disposed or reused.
- Removable media devices such as USB keys temporarily used to transfer data classified as Confidential or Sensitive between devices should be erased by using *(Specify how to erase USB keys. For example: using the USB eraser device located in the copy room)* as soon as possible after use.
- Servers, storage devices and computers storing Confidential or Sensitive information must be erased before releasing them to external third-party vendors for maintenance.
- IT equipment, systems and devices must be stored and used in temperature-controlled facilities with access to the area protected by locks and visitor management processes such as badges and/or staff escort.
- The data security processes will be reviewed annually as part of the Election WISP review prescribed in Policy 1.
- Data security processes must comply with all current or future information security federal and state regulations and laws, including the Texas Public Information Act, and the Records Management Retention and Disposition Schedules issued by the Texas State Library Archives Commission (TSLAC).

TABLE 2: ELECTION DATA CLASSIFICATION SYSTEM

DATA CLASSIFICATION LEVEL	DATA TYPE
Confidential	
Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.	• Written Information Security Program • Election Information Security Policy • Election System Security Plan • Cybersecurity Incident Response Plan • Continuity of Operations Plan • Vendor Risk Management Policy • Vendor Risk Assessment Results • Election Security Assessment (ESA) Results • Employee and Poll Worker Personally Identifiable Information and Financial Data • Election Department Critical Infrastructure Information • Polling Location Technology Configuration • Passwords, Including Login Credentials for All Systems and Election Devices • Vulnerability Scan Data • Threat Monitoring and Cyber Intelligence Information • System Inventory Information • System Life Cycle Management Information • Security Incident Reports or Event Details • Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including: o Social security number o Texas Driver License or TX Personal Identification Card Number o Indication that the applicant is interested in working as an election judge o Residence address of federal or state judges and their spouses o Residence address of applicants if the applicant or another person in the applicant's household is a victim of family violence, sexual assault or abuse, stalking or trafficking o Residence address of applicants participating in the address confidentiality program o Residence address of peace officers and other protected individuals under Texas Law.

	o Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity o Voter Registration Application Source Codes *For the full list and definitions of voter registration data that is confidential, refer to *Texas Election Code § 13.004 Recording and Disclosure of Certain Information by Registrar*
Sensitive	
Sensitive information is data that if altered or deleted could damage the interests of the organization or endanger the safety of citizens. This data can be made publicly available with approval, but it cannot be altered or deleted. It requires a higher than normal assurance of accuracy and completeness. It should be managed with integrity and security measures that ensure accuracy and appropriate availability.	• Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c) • Candidate Application Instructions • Poll Worker Instructions • Election Process Handbook/Guide • Voter Instructions • Candidate Information • Draft Ballot and Proof Information • Preliminary Tabulation Results • Vendor Information Excluding Vendor Risk Assessment Results • Password Management Policies • Technology Storage and Transportation Details • Escalation Path and Communication Plans for Suspected Security Incidents or Events • Roles and Responsibility Definitions and Assignments
Internal Use	
Internal Use information is data that is intended only for use within the Election Department. External access to this data should be prevented but disclosures are not critical. Internal access should be limited to only those individuals who require the data to perform their job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.	• Employee Handbooks • Security Awareness Training • Pollbook Technology Details • Background Check Processes • Vendor Information • Chain of Custody Documentation for Voting Systems and Ballots • Help Desk Instructions • Basic Facts About a Security Incident or Event o It Happened o It Is Being Addressed Rapidly o How It Impacts Voters
Public Use	
Public Use information is non-sensitive data that if distributed outside of the Election Department will not adversely impact the organization or citizens. This data has been	• Election News and Announcements • Job Announcements • Election System and Voting Equipment Types • Voting System Type • Poll Locations

declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.	- Election Schedules - Ballot Information - Tabulation Results - Official Domain URLs

POLICY 7: IDENTITY MANAGEMENT, AUTHENTICATION AND ACCESS CONTROL

Access to data, assets and facilities is limited to authorized users and follows the election data and asset classification systems if applicable.

POLICY STANDARDS

- Access to systems, computers and devices will be granted according to two classifications:
    - User - Granted to authorized personnel only.
    - Administrator – Administrator access must be approved by the (Specify the approval authority, such as Election Administrator.)
- Access to data and software must be assigned to users based on their roles to ensure each user only has access to the information required to perform job duties (See Appendix H).
- Shared user accounts are not permitted. A unique username is required for each user's access to systems, computers and devices as well as data and software functionality.
- All remote access sessions must use encryption and multifactor authentication when possible.
- Inactive user and administrator accounts will be disabled unless an exception is approved by the *(Specify the approval authority, such as Election Administrator.)*

POLICY 8: ELECTION INFORMATION SYSTEM MAINTENANCE

Maintenance and repairs of information system components should be performed regularly and logged. These systems include all voting technologies, ePollbooks, computers, and servers used to support elections.

POLICY STANDARDS

- Changes to election information systems and network architecture as well as chain of custody information must be tracked in the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log. An example is in the Appendix C.
- Preventative maintenance will be performed at a frequency that is equal to or greater than that suggested by the manufacturer and maintenance procedures will be documented in the Technology Asset Inventory, Classification, Chain of Custody and Change Management Log. An example is in the Appendix C.
- Systems removed from the network for maintenance and repair, either onsite or at an offsite facility, must be tested after the services are completed by running an anti-virus scan before they can be reconnected to the network.
- Maintenance agreements through third-party contracts must follow the Vendor Risk Management Policy.
- Maintenance performed by third parties on information systems via remote access tools must be monitored via screen sharing for the duration of the remote session.
- Annual network penetration testing is required. During years in which an Election Security Assessment is conducted, the penetration test performed as part of the assessment satisfies this requirement.
- Annual vulnerability scanning is required for all assets connected to the network. The vulnerability scan performed as part of an Election Security Assessment satisfies this requirement.

POLICY 9: USE OF PROTECTIVE TECHNOLOGY

Technology is used to prevent unauthorized access to data or technology, malware and ransomware infection and to secure information systems against disruptions, cyberattacks and equipment failure.

POLICY STANDARDS

- Email is protected by SPAM and malware filters.
- Internet content filtering should be used to block access to sites with potential viruses.
- An Endpoint Protection Solution should be used to protect computers, devices and systems from malware, ransomware and unauthorized access.
- Next-generation firewalls with encryption capabilities should be used to protect the network.
- Network segmentation must be implemented to separate critical election data sets and functionality from non-elections segments of the network and other department networks.
- Systems and devices must be configured with the least amount of functionality needed to perform assigned tasks to ensure that each user does not have more capability or than needed.
- All personal devices including USB drives, smartphones, cameras and music players must never be connected to the network unless approved by the *(Specify the approval authority, such as Election Administrator* and devices must be managed in compliance with the Removable Media Policy.

POLICY 10: INFORMATION SECURITY AWARENESS TRAINING

Personnel and partners participate in cybersecurity awareness training to ensure everyone understands their information security-related responsibilities and how to protect election data and technology.

POLICY STANDARDS

- Each member of the election staff is required to participate in the training offered by the Texas Secretary of State.
- Training for new users will take place no less than 30 days from their hire date and repeated annually thereafter.
- In addition to the general security content, training will include the Election WISP, including the Election Security Incident Response Plan, Continuity of Operations Plan, Data and Asset Classification Systems, Removable Media Policy and Security Roles and Responsibilities as well as any information relevant to specific roles.
- *(Specify the approval authority, such as Election Administrator)* must lead frequent discussions about security practices with the team to build a culture of physical and cybersecurity.
- Training records must be retained with human resources files for the amount of time allotted in the record retention requirements.

SECTION 3: DETECT

POLICY 11: CONTINUOUS SECURITY MONITORING

Network traffic, assets and physical access are monitored to identify cyberattack activities and verify the effectiveness of protective measures.

POLICY STANDARDS

- Monitoring must be conducted either internally or by contracting with a service to monitor and detect possible cyberattack activities across potential attack points including:
  - Network
  - Mobile access to the network
  - Third-party vendor interactions with the network and connected systems
- Monitoring activity must be conducted to detect unauthorized:
  - Connections
  - Devices
  - Software
  - Personnel
  - Code
  - Mobile access

POLICY 12: DETECTING ANOMALIES AND EVENTS

User behaviors and network traffic patterns that fall outside the normal pattern of activity must be identified quickly and analyzed to determine if these anomalies indicate a cyberattack.

POLICY STANDARDS

- As part of the monitoring process, normal network activity should be documented and used as a comparison point to detect anomalous activity that could indicate a security incident.
- The Election Security Incident Response Plan should document the activity that indicates an active attack and triggers activation of the Election Security Incident Response Plan.
- The impact potential of cyberattacks is determined and included in the Election Security Incident Response Plan to ensure that it is understood by personnel.

POLICY 13: DETECTION PROCESSES

Election and IT staff members are required to be vigilant in recognizing unusual activity that could be an indicator of a cyberattack, and suspicious activity must be immediately reported.

POLICY STANDARDS

- Election staff threat detection responsibilities are clearly defined to ensure staff know what they are expected to do to identify, report, and assist in the response to potential cyber threat activity. See the Election Security Roles and Responsibilities worksheet in Appendix B.
- Potential incidents must be reported immediately to *(Specify the approval authority role, such as Election Administrator).*
- The effectiveness of staff detection processes and Security Roles and Responsibilities must be reviewed annually as part of the Election WISP review prescribed in Policy 1. An example of the Security Roles and Responsibilities is in the Appendix A.
- Training staff on detection responsibilities and processes must be included in the Security Awareness Training required in Policy 10.
- Anti-virus software must be installed on laptops and devices that are in operation at all times. Staff must notify *(Designate a role within IT who is continuously available or an election staff role, such as the Election Administrator, with authority to notify the appropriate state resources if your organization does not have day-to-day IT support.)* of a high volume of blocked attack alerts.

SECTION 4 OBJECTIVE: RESPOND

POLICY 14: RESPONSE PLANNING

An up-to-date and authorized Incident Response Plan is maintained, made available to staff and followed in the case of a security incident.

POLICY STANDARDS

- An Election Security Incident Response Plan should be annually updated and maintained as part of the approved Election Written Information Security Program as defined in Policy 1.
- The Election Security Incident Response Plan includes processes to identify, contain, and eradicate active incidents as well as recover and implement improvements after the incident.
- The Election Security Incident Response Plan should be stored in digital and printed format with the other Election WISP documents as descripted in Policy 1.
- Information Security Awareness Training as defined in Policy 10 must include the Election Security Incident Response Plan.
- The Election Security Incident Response Plan should be added to the local government Emergency Response Plan.
- An Incident Response Team must be formally created with clearly described roles and responsibilities in the Election Security Incident Response Plan. The team should include *(Specify the roles that should be on the team such as the Election Administrator, Head of IT, Emergency Management Leadership and the Communications Director,)*, and members of the team should always be familiar with the plan and ready to respond to an incident.
- The Election Security Incident Response Plan must define incident preparation and all preparedness activities must be completed including gathering needed information in a single location and assembling equipment and resources that will be needed to respond to an incident.
- Every two years, Table-Top Exercises should be conducted that simulate an active incident so as to provide election staff with practice in executing the Election Security Incident Response Plan.

POLICY 15: ANALYSIS

Each security incident is analyzed to determine severity and scope and to ensure the right resources and stakeholders are assembled to address the full impact of the incident.

POLICY STANDARDS

- The Election Security Incident Response Plan must include a process for analyzing the cause and impact of an incident in consideration of the fact that some cyberattacks will be further reaching and more severe than others.
- Incidents should be categorized based on the severity of their impact on operations to guide the scope of response efforts.
- The analysis must include a review of potential third-party involvement to determine if response activities should incorporate third-party incident response policies and stakeholders.
- Evidence must be preserved to provide a court of law or cybersecurity insurance providers with needed information for prosecution and handling insurance claims. Evidence should be retained according to the duration specified for records retention in the election code.
- Using the information collected in the Incident Handler's Log included in the Election Security Incident Response Plan, an incident report must be completed for each incident that falls into the severity categories of Critical and High and submitted to the Texas Secretary of State Office.

POLICY 16: MITIGATION OF CYBERATTACKS

Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

POLICY STANDARDS

- Incidents must be immediately blocked and contained according to the processes outlined in the Election Security Incident Response Plan.
- As soon as an active incident is confirmed, the *(Specify the role with notification authority such as the Election Administrator)* must notify all election staff members and assemble the Incident Response Team according to the notification process defined in the Election Security Incident Response Plan.
- The Incident Response Team must immediately follow the mitigation steps outlined in the Election Security Incident Response Plan.
- The damage caused by an incident must be repaired as soon as possible, with priority recovery given to the mission statement and critical operations list defined in Policy 2.
- Backup data should be available and used to restore functionality and operations as described in the Election Security Incident Response Plan.

POLICY 17: RESPONSE COMMUNICATIONS

Response activities are coordinated with internal and external stakeholders including law enforcement agencies, insurance providers, IT service providers and public relations resources as defined in the Election Security Incident Response Plan.

POLICY STANDARDS

- A communication plan is included in the Election Security Incident Response Plan and Continuity of Operations Plan that encompasses both internal and external communications during a cyberattack incident.
- Each stakeholder must receive only the information they are authorized to receive according to Election Data Classification System defined in Policy 6.
- The communication plan should be aligned with information-sharing guidance from the public affairs office, legal department and leadership officials. As these entities make changes to their information-sharing guidelines, the Election Security Incident Response Plan must be updated to incorporate the new information.
- Public-facing communication about the incident should be distributed only through official election sources, such as the Election Authority's website. Press should be advised to only report ~~only~~ information that can be confirmed with the official Election Authority website.
- Social media should not report detailed information to avoid followers changing information as they share it. Social media should only direct followers to the Election Authority's website for all information.
- Clearly defined communication roles and responsibilities must be included in the Election Security Roles and Responsibilities list. An example is in the Appendix A.
- Incidents must be reported as required by laws and regulations which are defined in the Election Security Incident Response Plan.

POLICY 18: RESPONSE IMPROVEMENTS

Response procedures in the Election Security Incident Response Plan must be continuously improved by incorporating lessons learned from real and practice incident detection and response activities.

POLICY STANDARDS

- The Incident Response Team should meet one month or less after a security incident occurs or Table-Top Exercises have been completed to provide input and feedback on lessons learned.
- New practices or cyberattack defenses that emerge from the lessons learned must be added to the Election Security Incident Response Plan, the Continuity of Operations Plan and any other plans or policies in the Election WISP, as needed.
- If significant changes to any of the documents in the Election WISP are required to address response lessons learned, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by *(Specify the authorizing role such as Commissioner or Election Administrator.)*

SECTION 5 OBJECTIVE: RECOVER

POLICY 19: RECOVERY PLANNING

Recovery processes and procedures should be executed and maintained to ensure timely restoration of systems or assets affected by cyberattacks.

POLICY STANDARDS

- The Continuity of Operations Plan (COOP) must be followed immediately during a cyberattack to minimize disruption and continue to serve our mission.
- The recovery activities in the Election Security Incident Response Plan must be followed to enable a return to normal operations as quickly as possible.
- Recovery activities in all plans and policies should be reviewed at a minimum annually as part of the Election WISP review prescribed in Policy 1, and more frequently if needed after a Table-Top Exercise and after a cyberattack.
- Following significant changes made to organizational structure, election processes and technology infrastructure, the Election WISP should be updated with recovery activities aligned to the new information. Significant changes are those that add or remove resources and assets that must be protected from cyberattack and restored if they are disrupted by an attack.
- If significant changes to any of the documents in the Election WISP are required to address new or different recovery activities, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by *(Specify the authorizing role such as Commissioner or Election Administrator.)*

POLICY 20: RECOVERY IMPROVEMENTS

The recovery procedures in the Election Security Incident Response Plan and the Continuity of Operations Plan must be continuously improved by incorporating lessons learned from incident recovery activities.

POLICY STANDARDS

- The Incident Response Team should meet one month or less after a security incident occurs or Table-Top Exercises have been completed, to provide input and feedback on lessons learned in executing recovery activities.
- New or obsolete recovery practices that emerge from the lessons learned must be added to the Election Security Incident Response Plan, the Continuity of Operations Plan and any other plans or policies in the Election WISP as needed.
- If significant changes to any of the documents in the Election WISP are required to address recovery lessons learned, particularly changes that require additional resources and funding, the updated plan or policy should be approved and authorized by *(Specify the authorizing role such as Commissioner or Election Administrator.)*

POLICY 21: RECOVERY COMMUNICATIONS

Restoration activities should be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of affected systems, particularly systems spreading malware or other attack damage, additional victims and vendors.

POLICY STANDARDS

- A recovery communications plan must be a component of the Election Security Incident Response Plan to facilitate both internal and external communications during and after a cyberattack. The communications plan should ensure that each group of internal and external stakeholders only receives the information they are authorized to receive as defined in the Data Classification System in Policy 6.
- Public-facing communication about the recovery should be distributed only through official election sources, such as the website. Press should be advised to report only information that can be confirmed with the official Election Authority's website.
- Social media should not report detailed information to avoid followers changing information as they share it. Social media should only direct followers to the Election Authority's website for information.
- The communications plan should include public relations management after the cyberattack itself and then again after recovery. These two intervals of communication allow your entity to correct misinformation and to repair trust that may have been damaged during the incident.

APPENDIX A: ROLES AND SECURITY RESPONSIBILITIES

Role	Security Responsibility
Election Administrator	• Ensure the Election WISP is accessible only to election staff and all employees know where to find it and how to access it. • Ensure the Election WISP is approved and authorized by leadership. • Coordinate Election WISP reviews and updates in December after an election and in June after a legislative session. • If new cyber threats are identified, ensure that Election WISP policies and plans are updated with practices that protect against them. • Notify IT or cybersecurity resources of any reports from staff of suspicious activity or events that could indicate an active attack incident. • Notify the Texas Secretary of State Election Team if the activity is determined to be a true threat that requires activation of the Election Security Incident Response Plan. • Notify the Texas Department of Information Resources if the activity is determined to be a true threat. • Conduct an annual review of changes to operations and if the changes introduce new opportunities for cyberattacks. • Ensure that the most current version of the Election WISP is covered in the mandatory annual employee security awareness training curriculum.
All Election Staff	• Remain vigilant for indicators of a cyberattack. • Report suspicious activity to the Election Administrator who will immediately notify IT and/or security resources to determine if the activity indicates an active cyber threat. • Annually participate in security awareness training and Table-Top Exercises. • Know where to find the Election WISP. • Be familiar with the Election WISP and understand what to do to help protect operations, data and systems and how to respond to an incident. • Follow news about security threats and cybercrime trends and understand their potential impact to your elections.

Supply Manager	• Ensure that vendor contracts include the requirement to follow the Election Information Security Policy and the Vendor Risk Management Policy. • Ask vendors to provide security assessment results that include their security policies, plans and practices and store them with the vendor contract. • If a vendor is not following the Vendor Risk Management Policy, provide a reasonable timeframe to establish compliance. If the policy is still not being followed after the time period ends, consider changing vendors to engage with a vendor with the needed security practices.
Office Manager	• Maintain an up-to-date inventory of assets. • Require that visitors to the facility sign into a visitor log book, have name tags, and are escorted by staff. • Ensure that facilities are locked, and surveillance camera video is properly recorded and stored according to retention policies.
IT Manager	• Implement the data security requirements in the Security Best Practice Guidelines, Election Information Security Policy and the Election Systems Security Policy. • Monitor cyber intelligence feeds from MS-ISAC/EI-ISAC and the media for cyber threat trends that could impact elections and require defense adjustments.
Voter Registrar	• Adhere to the Election Information Security Policy and the Elections Systems Security Policy. • Report suspicious activity to the Election Administrator who will immediately notify the appropriate entities to determine if the activity indicates an incident. • Annually review changes to the voter registration process and determine if the changes introduce new opportunities for cyberattacks that require additional or new security practices or render some existing practices obsolete. • Communicate voter registration process changes to the Election Administrator and request that the changes be incorporated into Election WISP if needed.
Tax Collector	• Adhere to the Election Information Security Policy and the Elections Systems Security Policy. • Report suspicious activity to the Election Administrator who will immediately notify the appropriate entities to determine if the activity indicates an incident. • Annually review changes to the tax collection process and determine if the changes introduce new opportunities for cyberattacks that require additional or new security practices or render some existing practices obsolete.

	- Communicate tax collection process changes to the Election Administrator and request that the changes be incorporated into the Election WISP if needed.

APPENDIX B: THREAT AND RISK MONITORING LOG

MONITORING FREQUENCY: WEEKLY	ASSIGNED TO: IT Manager
MONITORING SOURCES: MS-ISAC/EI-ISAC ALERTS, MEDIA CHANNELS	REPORT SIGNIFICANT FINDINGS TO: Election Administrator and Texas DIR
POLICY UPDATE FREQENCY: TWICE/YEAR OR WHEN SIGNIFICANT THREATS EMERGE	POLICY UPDATE APPROVAL BY: Election Administrator

Identified Risk	Potential Impact (including operations, assets and individuals)	Security Measures Implemented	Policy Update Section and Date If Required	Logged By, Date	Source
URL Hijacking	Threat actors can disseminate false information to disrupt an election or disparage a candidate	Work with Texas Department of Information Resources to claim ownership of related domain names and shut down fake sites		Bill Parks 10.14.18	CNN News Article: *The Wild Wild Web* 10.12.18
Disinformation Campaigns	Threat actors or citizens intent on swaying elections can influence online discussions and plant media stories with false information.	Emphasize to citizens that all official election information will be posted only on the official website	Incident Response Plan Section 10.2	Bill Parks 6.3.19	MS ISAC
Cryptolocker Ransomware	Once it infects one system, it can self-	End-point security solution and		Bill Parks 8.24.19	ICMA Conference Session

	propagate across all systems in the network taking down the technology needed to conduct an election.	educate staff on not clicking on links or opening attachments from unknown sources.			

APPENDIX C: TECHNOLOGY ASSET INVENTORY, CLASSIFICATION, CHAIN OF CUSTODY AND CHANGE MANAGEMENT

TECHNOLOGY ASSET INVENTORY, CLASSIFICATION, CHAIN OF CUSTODY,CHANGE MANAGEMENT LOG

ASSET GROUP: OFFICE EQUIPMENT

INVENTORY				CHAIN OF CUSTODY				CHANGE MANAGEMENT LOG				
Security Level (Refer to Asset Criticality System)	Connected to Network?	Asset Model, Type and Serial or Product Number	Location and Critical Operation Support if Applies	Issued To/Date	Issued By	Returned To/Date	Retire Date/ Date Erased?	Maintenance, Change, Patch, Update/Date	Date Given to Technician / Technician Name	Location change was made	Confidential and Sensitive Data Removed Before Moving Offsite?	Date Returned to User
3	Yes	Dell XPS Laptop 12345678-9101	Room 11C, Election Management	Bill Parks/ 10.11.16	Mary Gilchrist			Upgraded OS /12.6.17	12.6.17/ Mary Gilchrist	Room 8b	N/A	12.6.17
								Screen Repaired/ 4.22.18	4.19.18/ Sam Fisher	Offsite CompuTech	Yes	4.23.18
3	Yes	Canon Printer/Copier 8765483	Courthouse Supply Closet	All Staff/ 7.8.17	N/A	N/A		Onsite Cleaning & Maintenance/ 8.10.18	N/AABC Business Supply	Copy room	N/A	N/A

APPENDIX D: REMOVABLE MEDIA POLICY

Overview

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. As an Election Authority, it is imperative that every removable media device be tightly controlled and properly used in order to protect the integrity of the election process.

2.0 Purpose

The purpose of this policy is to minimize the risk of loss or exposure of sensitive election information and to reduce the risk of acquiring malware infections on computers. Any questions or comments about this policy should be directed to the [EX: Election Administrator].

3.0 Scope

This policy covers all removable media that contains election data or that is connected to the secure network.

4.0 Policy

Staff may only use specifically approved removable media devices on any system or network related to an election or to any election process. Each media device must be properly noted in the inventory logs and an IT administrator must make changes to the Election Secure Network to allow computers to access the removable media device.

Any other removable media use must be approved by leadership and requires the use of an encrypted USB device that uses FIPS 140-2 approved encryption levels. The following devices are specifically approved for use:

[EX: Encrypted USB Drives

Encrypted External Hard Drives]

No exceptions to this policy are allowed.

5.0 Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment.

6.0 Definitions

Removable Media

Removable media is defined as devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and software disks.

Encryption

Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process. Encryption is provided in various forms, some of which are more secure than others. In order to ensure a suitable level of encryption, users are required to only use devices that are approved by the federal government with a FIPS 140-2 level of encryption.

Malware

Malware is defined as software of malicious intent/impact such as viruses, worms, and spyware.

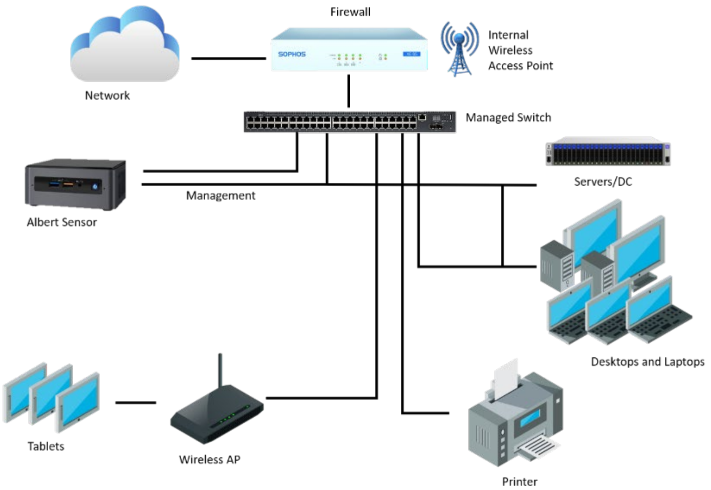
Sensitive Information

Sensitive information is defined as information which, if made available to unauthorized persons, may adversely affect the election process Examples include, but are not limited to, voter data, election processes, unreleased election data, personal identifiers and financial information.

APPENDIX E: NETWORK TOPOLOGY DIAGRAM

A network topology diagram doesn’t have to be complex. The main objective is to create a visual representation of how each system connects to other systems. This can be simply drawn out on a piece of paper, or it can be created using PowerPoint. This diagram was created using PowerPoint and icon graphics.

Example Network Topology Diagram



Insert Network Topology Diagram Here

APPENDIX F: DATA INVENTORY AND CLASSIFICATION

Critical Operation Support	Data Classification	Data Type	Location	Connected to Network	Access Permission
Voter Registration	Confidential	Voter Personal Identifying Information (PII)	TEAM	Yes	Voter Registrar, Election Administrator, Poll Workers
Human Resources	Confidential	Employee Personal Identifying Information (PII)	ADP	Yes	Staff Members

APPENDIX G: ACCESS PERMISSIONS

Asset	User	Admin	User and Admin
TEAM Voter Registration System	Poll workers Election Administrator Office Manager		Registrar
Candidate Database		IT Director	Election Administrator
Website	Election Administrator	IT Director	Communications Director
ePollbooks	Poll workers		Election Administrator
Employee Laptops	Employee	IT Director	
Security Incident and Event Management System			IT Director
Firewall			IT Director
Payroll Portal	Employees	IT Director	Human Resources Director
Social Media Channels	Election Administrator		Communications Director

ELECTION SECURITY BEST PRACTICES GUIDE

TEXAS SECRETARY OF STATE

ELECTIONS DIVISION

www.sos.texas.gov ∗ www.votetexas.gov
1.800.252.8683

(Last Revised: April 2020)

INTRODUCTION

To protect elections throughout the state from **cyber threats**, HB 1421(2019) requires the Texas Secretary of State (SOS) to adopt rules defining classes of protected election data and establishing best practices for identifying and reducing risk to the electronic use, storage and transmission of election data and the security of election systems.

The best practices prescribed in this document were developed by reviewing aggregate findings from the Election Security Assessments (ESAs) of county election offices that were conducted as required by HB 1421, reviewing election security documentation published by the Center for Internet Security and the State and Local Election Security Playbook by Belfer Center, the National Institute for Standards and Technology Cybersecurity Framework, and consultation with select election security experts.

This **Election Security Best Practices Guide** is intended to help Election Authorities, defined as any organization that holds responsibility for conducting elections, by providing guidance on address cyberattack and other disaster risks that the Internet introduces to the election process. Defending elections not only involves protecting voting machines and ballots, but also protecting the functions and technologies that support election processes and manage voter and election result data. While most of the recommendations are directed towards county election offices, these best practices could apply to any entity and individual with a role in conducting elections or managing election-related data before and after elections.

Recognizing that election security must take an all-encompassing, holistic approach, the best practices encompass security issues related to:

- The full election process:
  - Election Process Management
  - Election Staff Support
  - Voter Registration
  - Ballot Creation
  - Voter Check-In
  - Vote Capture
  - Vote Tabulation
  - Election Night Results Reporting
- Physical access to facilities that house election-related technology
- Integrity measures that apply to how staff and volunteers handle information throughout the election process
- Computer workstations and servers
- Devices that access the **network** and Internet such as electronic pollbooks, computers, servers, printers and peripheral devices
- The organization's technology **infrastructure**

It is important to note that these guidelines **do not apply directly to any specific voting machine and tabulation system equipment manufacturer types,** and do not supersede or otherwise replace the various election processes identified in the Texas Election Code, the Texas Administrative Code and Texas Secretary of State Elections Division Advisories.

It is recommended that Election Authorities review this Election Security Best Practices Guide in its entirety with all personnel, Information Technology (IT) teams and other election support teams. The purpose of the review is to determine if current election processes and technology management and use, including items relevant to external vendors and suppliers, follow these cybersecurity best practices. In this way, election authorities can use the guide to identify any security measures that should be put in place.

ORGANIZATION OF ELECTION SECURITY BEST PRACTICES GUIDE

The Election Security Best Practices Guide is broken into two parts. First, we have defined the different classes of election data and provided some general guidelines as to how to develop policies related to securing these data classifications. Second, after defining the classes of election data, we provide the list of best practices. The best practices have been broken into four general categories: **(1) Policy and Processes, (2) Election Processes, (3) Network and IT Infrastructure, and (4) Supporting Technology.**

Within each category, the Election Security Best Practices Guide separates the recommendations into two levels according to their criticality to help Election Authorities prioritize the implementation of the practices: **(1) Priority Best Practices** and **(2) Standard Best Practices**. Priority Best Practices are urgently critical and form the foundation of election cybersecurity. **It is recommended that Election Authorities consider it an imperative priority to implement, at a minimum, the Priority Best Practices.** After achieving the **Priority Best Practices**, election officials should then work on implementing the **Standard Best Practices** which will assist election officials in moving closer to the optimum level of cybersecurity readiness for elections.

This document also includes a summary of the data classifications in **Appendix A** and a prioritized checklist in **Appendix B** that presents the best practices in a summarized format to help Election Authorities track the progress of their election security implementation efforts. Additionally, we've included a glossary in **Appendix C** with definitions of the technical terms used throughout the document.

TEXAS SOS RESOURCES TO HELP IMPROVE ELECTION SECURITY

To assist election officials in adhering to the best practices provided, the Texas SOS has hired election security trainers to provide election officials with individual guidance on how to meet the best practices prescribed. The trainers can also direct election officials to free and low-cost resources that are available to assist with implementing both priority and standard best practices.

Additionally, we have created a **Texas Election Security Toolkit** to help Election Authorities secure their elections. The election security trainers can provide access to the toolkit and can guide election officials in completing the templates in a way that meets their county needs and adheres to prescribed best practices. Including this document, the toolkit consists of a total of six guides:

1. Election Security Best Practices Guide
2. Election Information Security Policy Template
3. Election Incident Response Plan Template
4. Election Continuity of Operations Plan Template
5. Election System Security Plan Template
6. Election Vendor Risk Management Policy Template

Within each guide, we reference the best practices to show which are being addressed when completing different portions of the guides.

The election security trainers are available to work individually with a county or to provide regional trainings on the information contained in the Election Security Toolkit as well as on other general election security topics. To contact our election security trainers or to get access to the Texas Election Security Toolkit, please email electionsecurity@sos.texas.gov with your requests.

Part 1 - DATA CLASSIFICATIONS LEVELS

As Election Authorities develop security policies, plans and processes, data classification levels for voter and election data provide a helpful framework. Data classification ensures that security practices are aligned to the required protections for each data type and how the information is used.

Below you will find four recommended classification levels: **(1) Confidential, (2) Sensitive, (3) Internal Use, and (4) Public Use**. You will notice that there is some overlap between the types of data included in each category. This is intended to give you options depending on how your organization uses and stores the data.

1. **Confidential:** Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is likely exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.
    a. **Confidential Data Categories:**
        1. Written Information Security Program
        2. Election Information Security Policy
        3. Election System Security Policy
        4. Cybersecurity Incident Response Plan
        5. Continuity of Operations Plan
        6. Vendor Risk Management Policy
        7. Vendor Risk Assessment Results
        8. Election Security Assessment (ESA) Results
        9. Employee and Poll Worker Personally Identifiable Information and Financial Data
        10. Election Department Critical Infrastructure Information
        11. Polling Location Technology Configuration
        12. Passwords, Including Login Credentials for All Systems and Election Devices
        13. Vulnerability Scan Data
        14. Threat Monitoring and Cyber Intelligence Information
        15. System Inventory Information
        16. System Life Cycle Management Information
        17. Security Incident Reports or Event Details
        18. Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including:
            a. Social security number
            b. Texas Driver License or TX Personal Identification Card number
            c. Indication that the applicant is interested in working as an election judge

d. Residence address of federal or state judges and their spouses
e. Residence address of applicants if the applicant or another person in the applicant's household is a victim of family violence, sexual assault or abuse, stalking or trafficking
f. Residence address of applicants participating in the address confidentiality program
g. Residence address of peace officers and other protected individuals under Texas Law.
h. Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity
i. Voter Registration Application Source Codes

*For the full list and definitions of voter registration data that is confidential, refer to *Texas Election Code § 13.004 Recording and Disclosure of Certain Information by Registrar*

2. **Sensitive:** Sensitive information is data that if altered or deleted could damage the interests of the organization or endanger the safety of citizens. This data can be made publicly available with approval from election official, but it cannot be altered or deleted. It requires a higher than normal assurance of accuracy and completeness. It should be managed with integrity and security measures that ensure accuracy and appropriate availability.
   a. **Sensitive Data Categories:**
      1. Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c)
      2. Candidate Application Instructions
      3. Poll Worker Instructions
      4. Election Process Handbook/Guide
      5. Voter Instructions
      6. Candidate Information
      7. Draft Ballot and Proof Information
      8. Preliminary Tabulation Results
      9. Vendor Information Excluding Vendor Risk Assessment Results
      10. Password Management Policies
      11. Technology Storage and Transportation Details
      12. Escalation Path and Communication Plans for Suspected Security Incidents or Events
      13. Roles and Responsibility Definitions and Assignments

3. **Internal Use**: Internal Use information is data that is intended only for use within the Election Department. External access to this data should be prevented but disclosures are not critical. Internal access should be limited to only those individuals who require

the data to perform their job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.

a. **Internal Use Data Categories:**

    1. Employee Handbooks
    2. Security Awareness Training
    3. Pollbook Technology Details
    4. Background Check Processes
    5. Vendor Information
    6. Chain of Custody Documentation for Voting Systems and Ballots
    7. Help Desk Instructions
    8. Basic Facts About a Security Incident or Event

        a. It Happened

        b. It Is Being Addressed Rapidly

        c. How It Impacts Voters

4. **Public Use**: Public Use information is non-sensitive data that if distributed outside of the Election Department will not adversely impact the organization or citizens. This data has been declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.

    a. **Public Use Data Categories**

        1. Election News and Announcements
        2. Job Announcements
        3. Election System and Voting Equipment Types
        4. Voting System Type
        5. Poll Locations
        6. Election Schedules
        7. Ballot Information
        8. Tabulation Results
        9. Official Domain URLs

Part 2 - ELECTION SECURITY BEST PRACTICES

Category 1: POLICIES AND PROCESS

1. **CREATE AN AUTHORIZED ELECTION WRITTEN INFORMATION SECURITY PROGRAM (WISP).** A WISP is a set of policies and plans that define how to protect elections from cyberattack and how to respond if an incident occurs. It authorizes employees to quickly perform the described actions without waiting for approval during an attack.

   a. Ensure that all policies and plans are authorized by the appropriate authorities and are officially adopted and implemented by the staff and IT teams.

   b. Review the plans and policies in the WISP at least once a year according to the following schedule:

      i. During general election years, in December after an election to incorporate any needed improvements and clarification identified during the election as well as new risks

      ii. During legislative session years, in July after the state election law conference to incorporate any new laws affecting elections as well as new risks

   PRIORITY BEST PRACTICES

   c. Create an **Election Information Security Policy.** The purpose of an Election Information Security Policy is to establish protocols that protect election-related data from cyber threats and other disasters.

      i. Develop a data classification system that can be used to establish the appropriate security needed for each data type. See Data Classifications in Part 1 for more guidance.

      ii. Organize the policy around the five security objectives established by the **National Institute of Standards and Technology (NIST)** Cybersecurity Framework (CSF): (1) Identify (2) Protect (3) Defend (4) Respond, and (5) Recover.

   d. Create an **Incident Response Plan** that documents the specific steps to take in case of cyberattack or other types of disasters.

      iii. An Incident Response Plan should include:

         1. A clear definition of what constitutes a cyberattack or incident
         2. A classification system for the severity level of incident types and the appropriate notification and response protocol for each type
         3. **Incident containment processes** that minimize the scale and scope of the damage
         4. Procedures for restoring systems and operations after an attack

      iv. An incident Response Plan should address, at a minimum, the following incidents:

         1. Malware
         2. **Ransomware**
         3. **Denial of Service (DoS) and Distributed Denial of Services (DDoS)**
         4. Intrusion
         5. Information access
         6. Compromised data

7. Insider threats
8. Compromised accounts
9. Loss or theft of election and/or computer systems
10. Social engineering attack
11. Data breach

e. Create a **Continuity of Operations Plan** (**COOP).** A COOP should consider how a cyberattack may disrupt an election and explain fail-safes, backup processes and systems to keep critical functions operating if a cyber incident occurs.

i. Align the COOP with the Incident Response Plan for consistency and clarity.

STANDARD BEST PRACTICES

f. Create an **Election System Security Plan**. An election system security plan provides written protocols that protect election-related equipment housing election data from cyber threats and other disasters. An Election System Security Plan should:

i. Describe job functions and the responsibilities of the roles that interact with each system.
ii. Define security controls that encompass the full scope of how election and IT systems support elections.
iii. Include the complete range of election processes from registering voters to reporting results.
iv. Identify how systems work together to accomplish each election function.
v. Outline how election equipment and systems are secured and stored.
vi. Include how voters interact with systems

g. Create a **Vendor Risk Management Policy.** A Vendor Risk Management Policy is a written policy that creates guidelines for an election office to ensure that third-party vendors are not introducing security gaps that bad actors can exploit to stage an attack. As part of the policy, election offices should request that their vendors:

i. Provide a copy of their Information Security Policies and Plans to determine whether the vendor practices reasonable security measures.
ii. Allow periodic evaluation and information gathering on how they protect information and systems.
iii. Have documented controls or procedures on how they secure USB devices and any associated removable media.
iv. Document how the vendor will support the organization during execution of the Continuity of Operations Plan.

2. MONITOR CONTINUOUSLY FOR THREATS

PRIORITY BEST PRACTICES

a. Contract an external security service provider to monitor the network and remote systems 24 hours every day and analyze events for indicators of cyberattack. Available services include:

i. Albert Sensor from the Center for Internet Security (CIS)
ii. Monitoring services available through the Texas Department of Information Resources (DIR)

b. Ensure the service provider uses effective threat monitoring software and hardware products, particularly a **Security Incident and Event Management (SIEM)** solution.

3. PERFORM VULNERABILITY SCANNING AND PATCH MANAGEMENT

PRIORITY BEST PRACTICES

a. Establish a monthly **patch management** process to address any operating system and software application vulnerabilities.

b. Conduct monthly **vulnerability scans** of all internal systems and maintain a log of recent scans. The log should include:

   i. Details about detected vulnerabilities

   ii. Records of any remediation steps taken to fix the vulnerability

4. CLASSIFY AND PROTECT ELECTIONS DATA

PRIORITY BEST PRACTICES

a. Review and Identify Confidential, Sensitive and Internal Use Data within the Elections environment as described in the Data Classification Guidelines.

b. Ensure that all Confidential, Sensitive and Internal Use data has these best practices applied appropriately, such as implementing encryption for Confidential Data and limit access to systems to only approved and authorized users.

c. Control which users have access to each class of elections data, through process and technology, where possible. Evaluate the roles of the staff and consider limitations such as:

   i. Confidential Data should be limited to the Election Authority and a very limited support team that requires access as necessary to conduct their job duties.

   ii. Sensitive Data should be limited to employees and Full-Time Elections staff.

   iii. Temporary election staff access should be limited to subsets of information where possible and have an account assigned to them individually so that access to data can be monitored.

4. PARTICIPATE IN SECURITY AWARENESS TRAINING

PRIORITY BEST PRACTICES

a. Each member of the election department staff is required to participate in the SOS cybersecurity training required by and provided by the Texas SOS Office.

b. Each staff member is required to repeat the security training annually

c. Election officials should discuss the security recommendations in the training videos with staff to create a culture of security awareness.

6. CONDUCT ELECTION SECURITY ASSESSMENTS REGULARLY

PRIORITY BEST PRACTICES

a. Participate in the Election Security Assessment provided by the Texas SOS Office as required by Section 279.003, Texas Election Code.

b. Conduct subsequent security assessments at least once every two to four years or more often if the political subdivision has a significant change in structure or circumstance such as purchasing new equipment, moving to a new office, or changing personnel. Certain political subdivisions may be eligible for assessments provided by DHS. Election authorities may also contract with private entities to conduct security assessments.

c. Use the ESA results and the results from any subsequent assessment to establish a roadmap defining how and when the required improvements will be made.

STANDARD BEST PRACTICES

d. Review the most recent ESA every year to ensure recommendations were effectively implemented, identify opportunities for improvement and maintain alignment with the roadmap.

e. Use the vendor risk management review included in the ESA to develop requirements for the Vendor Risk Management Policy.

7. PARTICIPATE IN THE DHS MS-ISAC AND EI-ISAC INFO SHARING PROGRAM

a. Election Officials should join the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) information services and IT officials should join the Multi-State Information Sharing and Analysis Center (MS-ISAC) and provided by the Department of Homeland Security (DHS).

b. Review communications and develop a process for monitoring the cyber threats tracked and reported by the MS-ISAC/EI-ISAC Security Operations Center (SOC)

Category 2 - ELECTION PROCESS

1. IMPLEMENT A TWO PERSON VERIFICATION PROCESS

PRIORITY BEST PRACTICES

a. Ensure that every election function from ballot programming to Election Night Reporting uses a two-person verification method in which one person performs the task and a second person witnesses and verifies the accuracy and integrity of the result.

b. Two-person verification should occur during:

- i. Ballot programming of electronic and paper ballots
- ii. Election device programming
- iii. Receipt of election media devices
- iv. Breaking and attaching tamper-evident seals
- v. Ballot counting
- vi. Tabulation of election results
- vii. Election Night Reporting of results

c. In accordance with the state election code information retention policy, keep a record with full signatures from the two people who participated in the verification process.

d. Work closely with election vendors to foster an environment of two-person verification.

2. ELECTION NIGHT REPORTING INTEGRITY

PRIORITY BEST PRACTICES

a. Only disseminate results to the public on election night through the organization's official website.

- i. Use email messages and social media posts to direct the public to the official website to view the election results.
- ii. Do not email results to certain parties or the media, and do not publish results through social media accounts.

STANDARD BEST PRACTICES

b. Include the following integrity validation measures on the website when publishing results:

- i. The organization's logo or seal on the document or a watermark in the document header or footer.
- ii. A file **checksum** value that can verify legitimate results. A free Microsoft utility can accomplish this. (https://support.microsoft.com/en-us/help/841290/availability-and-description-of-the-file-checksum-integrity-verifier-u)

iii. A statement that the results are unofficial until after the election canvass and post of the date of the canvass.

c. Remove previous unofficial results from the website once the official results are completed or move to a section of your website titled “historical results.”

d. Do not post unofficial or official reports printed from tabulation systems or results pages that include the election system vendor’s name.

3. DOCUMENT ELECTION PROCESSES

STANDARD BEST PRACTICES

a. Create an election handbook that captures the experience and expertise of key staff members to clearly outline the full scope of the election process.

b. Ensure that the handbook accomplishes key election department objectives such as:

i. Facilitating cross training between roles and departments

ii. Enabling the consistent implementation among staff members of election security best practices

iii. Understanding and following the Written Information Security Program’s plans and policies

4. PHYSICALLY SECURE ELECTION OFFICES AND SYSTEMS

PRIORITY BEST PRACTICES

a. Establish a chain of custody documentation process for election systems that includes:

i. The original source of the system

ii. When the system first arrived at the organization

iii. Who received the system

iv. Condition of the system

v. Where the system is stored

vi. When the election system is used in a different location, such as a polling site, document:

- Date
- Time
- Who issued the system
- Who received and transported the system
- The location where it was used

vii. When the system is returned to its storage location, document:

- Date
- Time
- Who transported and returned the system
- Who received the system
- Storage location

b. Never leave systems with network access unattended unless they are in a locked area.

c. Control physical access to election equipment at all times and utilize tamper evident seals for integrity protections, even when they are not in use for elections.

d. Set up a secure perimeter with functioning conventional or digital locks protecting all entry points.

e. Use trackable access codes or keycards if possible, or at minimum implement entry and exit logs to track entry to secure areas where election systems are located.

f. Identify all visitors to your election office

   i. Visitors should enter and exit in a controlled area.

   ii. Document time of arrival.

   iii. Provide visitor credentials to be displayed while in the secure area.

   iv. Require an escort by a member of the election staff at all times.

   v. Document the time of departure.

g. Use an access control key or password witnessed by one or more individuals when securing election equipment. Document the use of an access control key in a log dedicated for that purpose and have a witness sign the log.

h. Monitor all entry and exist points to election facilities with cameras that have recording capability and have security personnel patrol the area when possible. Review the camera footage if an incident occurs.

i. Adhering to the state election code information retention policy time requirements, keep all chain of custody documentation, camera footage and access logs documenting secure area entry/exit and access control key or password use.

Category 3 - NETWORK AND INFRASTRUCTURE

1. INSTALL A NEXT GENERATION FIREWALL

PRIORITY BEST PRACTICES

a. Install an **enterprise-class**, **next generation firewall (NGFW)** to segment election systems, functions and data from the rest of the network and strengthen Internet security. The next-generation firewall should include:

- **Network Segmentation** Capabilities
- **Stateful Deep Packet Inspection**
- **Virtual Private Network (VPN)** Support
- Web-traffic Filtering
- Intrusion Detection and Prevention System
- Application Inspection and Control
- Geolocation Blocking
- DoS, DDoS, and **Port Scan Blocking**

b. Configure the firewall to control outbound activity from election computers and to block unauthorized access to the network from the Internet or other network segments and networks that support the organization.

c. Check for firewall patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

2. SEGMENT THE NETWORK

PRIORITY BEST PRACTICES

a. Using a firewall or Next Generation Firewall, partition the network to create a section dedicated to election-related functions.

b. Protect access to this segment from the rest of the network, other networks or the Internet with its own firewall (see additional guidance on firewall implementation in the Network and Infrastructure section.)

c. Restrict access to the election segment of the network to only employees who need the data it contains to perform their job duties.

3. UPGRADE UNSUPPORTED END-OF-LIFE OPERATING SYSTEMS AND SOFTWARE.

PRIORITY BEST PRACTICES

a. Upgrade or replace operating systems earlier than Windows 10 Professional or Windows 10 Enterprise.

b. Ensure that the software installed on systems used to support elections is current and critical security patches are up to date.

c. Check for patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

4. RESTRICT NETWORK ACCESS

PRIORITY BEST PRACTICES

a. Limit remote access to the election network.

b. Tightly control management tools that grant remote access to a limited number of employees.

c. Permit only vendor connections that have been evaluated according to the Vendor Risk Management Policy.

d. Prohibit network access through internet access points or other connections that are not protected by the next-generation firewall.

5. USE ENDPOINT SECURITY SOLUTIONS

PRIORITY BEST PRACTICES

a. Prevent **endpoints** from enabling attackers to access the network by implementing Endpoint Security Solutions that detect and block threats. The solution should include:

   i. Anti-virus/Anti-malware

   ii. Ransomware protection

   iii. Host Intrusion Detection System (HIDS)

b. Deploy the solution on all endpoint devices, except systems provided for vote tabulation.

c. Check for patches and updates on a monthly basis in alignment with the Vulnerability Scanning and Patch Management best practice.

6. IMPLEMENT SOFTWARE AND NETWORK WHITELISTING

PRIORITY BEST PRACTICES

a. Configure each election system with software such as Endpoint Security Software or Windows 10 Enterprise that prohibits the execution of unapproved software packages including: Applications, Email, **Web Servers,** and Endpoint Devices.

b. Establish a process that requires approval for additional software package installations.

c. Protect access to the election network by preventing any unapproved devices from communicating with systems behind the firewall.

d. Disable unused **network ports** at the **network switch**.

e. Configure active ports to block access to unapproved devices and prevent unauthorized network access.

7. SECURE WIRELESS NETWORKS AND DEVICES

PRIORITY BEST PRACTICES

a. Disable or deactivate wireless devices (Wi-Fi and Bluetooth) that are not in use or defined in the acceptable use policy.

b. Separate (**network segmentation**) all other Wi-Fi networks from the election department's Wi-Fi network

STANDARD BEST PRACTICES

c. Create a policy that defines acceptable use of wireless devices.

d. Configure Wi-Fi networks to use **Wi-Fi Protected Access 2 (WPA2)** or later security controls that adhere to the Advanced Encryption Standard (AES).

e. Ensure that passphrases meet the minimum password standards.

f. Hide the election department's **Service Set Identifier (SSID).**

g. If Wi-Fi is used to support a polling place, restrict the wireless network to supporting only the required ePollbook functionality.

8. BACKUP DATA OFFSITE USING ENCRYPTION

PRIORITY BEST PRACTICES

a. Backup critical election data daily on encrypted backup drives or systems housed offsite. When using a computer system as backup, ensure that the system is not connected to the election network.

b. Backup all data that can be classified as Confidential, Sensitive or Internal Use (defined above) related to election activities.

c. Encrypt and store backup data using **FIPS 140-2 encryption** levels.

9. ENCRYPT ELECTION AND VOTER INFORMATION

PRIORITY BEST PRACTICES

a. Encrypt data storage for servers that support the election environment. All data that is classified as Confidential, Sensitive or Internal Use (as defined above) must be stored in an encrypted file system or system disk.

b. Require encryption for cloud solutions used to store Confidential, Sensitive or Internal Use information (such as voter registration applications or election management information).

STANDARD PRACTICES

c. Encrypt the hard disks of computer systems that access and process voter registration information or critical election data using an encryption product such as Windows BitLocker.

10. MANAGE REMOVABLE MEDIA USE

PRIORITY BEST PRACTICES

a. Create a **Removable Media** Policy as part of the Election Information Security Policy defining a list of approved media and their uses. Removable media includes USBs, Thumb drives, Memory sticks, Data cards and CDs.

b. For general purpose removable media use, allow only encrypted USB devices

c. Assign removable media device management to a single person

d. Keep a log to track removable media assignments and regulate their use at all times.

STANDARD BEST PRACTICES

e. Use software such as Endpoint Security Software or Windows 10 Enterprise that controls the use of specific removable media devices.

f. Supply and certify removable media devices such as USB keys or drives used by staff and ensure their use adheres to the Removable Media Policy.

g. Put removable media devices that transfer information between non-connected election systems through a USB cleaning process that deletes the contents on the device before they are stored or reused. Consider implementing a single-use policy for devices used to transfer data between non-connected systems where possible.

h. Delete contents and securely destroy single use removable media, such as write once DVDs (DVD-R), CDs (CD-R), and USB drives.

11. TRACK INVENTORY

PRIORITY BEST PRACTICES

a. Create a detailed inventory list of all technology used to support and conduct an election.

b. Maintain a digital and/or paper log of approved software and removable media devices that includes identifying features such as:

    i. Model
    ii. Serial number
    iii. Unique asset tag number
    iv. Location of deployment
    v. Person who issued the equipment
    vi. Person receiving returned equipment
    vii. Location of stored equipment

STANDARD BEST PRACTICES

c. Identify devices used for an election, including the identification of devices used during early voting separately from those used for Election Day and retained between elections.

d. When reusing a device, include a description of its contents before erasing the information and using the device again.

e. Keep inventory records for the amount of time specified in the applicable information retention policy.

Category 4 - SUPPORTING TECHNOLOGY

1. CONTROL AND PROTECT EMAIL AND WEBSITE DOMAINS

PRIORITY BEST PRACTICES

a. Election staff members should only use government-provided email addresses or web servers.

b. Counties should utilize official government domains ending in texas.gov or tx.us. Contact the Texas Department of Information Resources (DIR) for assistance in obtaining a texas.gov address.

c. Never perform election business from a non-government email address or website.

d. Implement a **Web Application Firewall (WAF)** for additional website security.

e. Update election website software with critical patches once per month.

STANDARD BEST PRACTICES

f. Perform a penetration test once a year for websites that provide election results or voter or election information

g. Ensure that all transmissions over election websites use a **Secure Socket Layer (SSL)** certificate that provides users with privacy and ensures that they are on the official website.

2. IMPLEMENT EMAIL SECURITY

PRIORITY BEST PRACTICES

a. Disable web-based internet access to email or require that Multi-Factor Authentication be used for web-based email access.

b. Integrate into your email system **Domain-Based Message Authentication, Reporting and Conformance (DMARC),** an email service that helps to identify legitimate email sources to prevent email spoofing, into your existing inbound email authentication process.

STANDARD BEST PRACTICES

c. Use multifactor authentication to control access to all email accounts

d. Implement SPAM filtering measures in the email server at the point of initial mail receipt.

e. Include anti-virus scanning of email messages to detect and block message attachments that contain viruses.

3. PASSWORDS AND MULTI-FACTOR AUTHENTICATION (MFA)

PRIORITY BEST PRACTICES

a. Require that every system used for election functions has a unique username for each individual staff member that is authorized to access the system.

b. Do not allow shared user accounts.

c. Use a Password Management Solution that stores passwords in an encrypted format and includes multifactor authentication to access.

d. Never write passwords down or keep them in locations that are accessible to others.

e. Never store passwords in spreadsheets, journals, or email contacts applications.

f. Update password policies on all systems to support the following complex password requirements:

   i. At least 12 characters

   ii. At least 1 upper case letter

   iii. At least 1 lower case letter

   iv. At least 1 number

   v. At least 1 special character

g. Force updates every 90 days

h. Enable multifactor authentication on Domain Administrator accounts.

i. Ensure that any system accessed remotely to support election processes uses multifactor authentication, including any election service provider portal or secure file transfer system.

STANDARD BEST PRACTICES

j. Implement Multi-Factor Authentication for all systems, internal and external, that support the election network or office.

k. Implement MFA solutions using soft tokens such as Microsoft Authenticator or Duo for the additional authenticating factor instead of text or email.

l. Discourage staff from sharing passwords or using joint accounts to any systems. If using a joint account is required, outline processes that detail security protocols to limit use.

m. Change system default passwords immediately after initial setup of a new system or device.

4. LIMIT ADMINISTRATOR ACCESS

PRIORITY BEST PRACTICES

a. Limit unauthorized access to endpoint computers and devices by configuring the Local Administrator account default settings during initial setup on all systems:

   i. Immediately change the default Local Administrator account password to a unique complex password.

   ii. Disable access to the Local Administrator account from the network.

b. Limit access to Domain Administrator accounts to authorized personnel only (typically the IT department) and require Multi-Factor Authentication for Domain Administrator accounts.

STANDARD BEST PRACTICES

c. Establish a user hierarchy based on the **Principle of Least Privilege** to ensure that users don’t have more access to administrative capabilities than they need to perform their job duties.

d. Establish an approval process for users who require **system or application administrator access** privileges, and never assign an administrative account to a user who does not require administrator-level control.

e. Ensure that administrators use a user account with end-user level permissions for routine operations and a separate administrator account for privileged administrative tasks.

APPENDIX A: DATA CLASSIFICATION CHART

TABLE 2: ELECTION DATA CLASSIFICATION SYSTEM

DATA CLASSIFICATION LEVEL	DATA TYPE
Confidential	
Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.	• Written Information Security Program • Election Information Security Policy • Election System Security Plan • Cybersecurity Incident Response Plan • Continuity of Operations Plan • Vendor Risk Management Policy • Vendor Risk Assessment Results • Election Security Assessment (ESA) Results • Employee and Poll Worker Personally Identifiable Information and Financial Data • Election Department Critical Infrastructure Information • Polling Location Technology Configuration • Passwords, Including Login Credentials for All Systems and Election Devices • Vulnerability Scan Data • Threat Monitoring and Cyber Intelligence Information • System Inventory Information • System Life Cycle Management Information • Security Incident Reports or Event Details • Protected Voter Registration Application Information including items Defined in Election Code 13.004 (c) including: o Social security number o Texas Driver License or TX Personal Identification Card Number o Indication that the applicant is interested in working as an election judge o Residence address of federal or state judges and their spouses o Residence address of applicants if the applicant or another person in the applicant's household is a victim of family violence,

	sexual assault or abuse, stalking or trafficking ○ Residence address of applicants participating in the address confidentiality program ○ Residence address of peace officers and other protected individuals under Texas Law. ○ Voter Registration Data Disclosing Criminal History or Voter Activity/Inactivity ○ Voter Registration Application Source Codes *For the full list and definitions of voter registration data that is confidential, refer to *Texas Election Code § 13.004 Recording and Disclosure of Certain Information by Registrar*
Sensitive	
Sensitive information is data that if altered or deleted could damage the interests of the organization or endanger the safety of citizens. This data can be made publicly available with approval, but it cannot be altered or deleted. It requires a higher than normal assurance of accuracy and completeness. It should be managed with integrity and security measures that ensure accuracy and appropriate availability.	• Voter Registration Data Excluding Criminal History, Voter Activity/Inactivity and Data Defined as Confidential in Election Code 13.004 (c) • Candidate Application Instructions • Poll Worker Instructions • Election Process Handbook/Guide • Voter Instructions • Candidate Information • Draft Ballot and Proof Information • Preliminary Tabulation Results • Vendor Information Excluding Vendor Risk Assessment Results • Password Management Policies • Technology Storage and Transportation Details • Escalation Path and Communication Plans for Suspected Security Incidents or Events • Roles and Responsibility Definitions and Assignments
Internal Use	
Internal Use information is data that is intended only for use within the Election Department. External access to this data should be prevented but disclosures are not critical. Internal access should be limited to only those individuals who require the data to perform their	• Employee Handbooks • Security Awareness Training • Pollbook Technology Details • Background Check Processes • Vendor Information • Chain of Custody Documentation for Voting Systems and Ballots • Help Desk Instructions • Basic Facts About a Security Incident or Event

job duties. Data in this category may become available to the public, if a public information request or inquiry is received and approved.	○ It Happened ○ It Is Being Addressed Rapidly ○ How It Impacts Voters
Public Use	
Public Use information is non-sensitive data that if distributed outside of the Election Department will not adversely impact the organization or citizens. This data has been declared public knowledge by someone with the proper authorization and should not be used or disclosed without approval.	• Election News and Announcements • Job Announcements • Election System and Voting Equipment Types • Voting System Type • Poll Locations • Election Schedules • Ballot Information • Tabulation Results • Official Domain URLs

APPENDIX B: BEST PRACTICE CHECKLIST

ELECTION SECURITY BEST PRACTICES CHECKLIST	PRIORITY BEST PRACTICES **Complete First**	STANDARD BEST PRACTICES After Implementing Priority Practices
	POLICIES AND PROCESS	
Create WISP (Written Information Security Program)	□ Ensure policies and plans are authorized □ Review yearly by appropriate personnel □ Create Election Information Security Policy □ Create Incident Response Plan □ Create Continuity of Operations Plan	□ Create Election System Security Plan □ Create Vendor Risk Management Policy
Monitor Continuously for Threats	□ Establish 24/7 security monitoring services □ Ensure provider uses effective products including a SIEM.	
Perform Vulnerability Scanning	□ Establish a monthly patch management process □ Conduct monthly vulnerability scans	
Classify and Protect Elections Data	□ Assign election data to data classification categories □ Apply appropriate protections for each data classification category □ Give users access to only the least amount of data needed for their role	
Participate in Security Awareness Training	□ Each member of the election staff is required to participate in the SOS cybersecurity training □ Repeat security training every year □ Discuss security recommendations with staff	
Conduct Election Security Assessments (ESAs) Regularly	□ Participate in the ESAs provided by Texas SOS	□ Use ESA results to establish an improvement roadmap □ Review ESA results yearly

	□ Conduct follow-up assessments at least once every two to four years (or more often if necessary)	
Participate in the DHS MS ISAC and EI ISAC Info Sharing Program	□ Become a member of the MS-ISAC/EI-ISAC □ Develop a process for monitoring the cyber threat reports	
	ELECTION PROCESS	
Implement a Two-Person Verification Process	□ Ensure that one person performs the task and a second person witnesses and verifies result integrity for every election function □ Keep a record with full signatures from both people □ Encourage election vendors to implement two-person verification □	□ Use integrity validation measures on the website when publishing results □ Do not post unofficial or official reports printed from tabulation systems or that include the election vendors name
Election Night Reporting Integrity	□ Only disseminate results to the public on election night through the official website □ Do not email results to external parties or the media □ Do not publish results through social media accounts Use email and social media to direct the public to the official website to view election results	
Document the Election Process		□ Create an election handbook that captures the experience of key staff members □ Ensure the handbook accomplishes key election department objectives
Physically Secure Election Offices and Systems	□ Establish a chain of custody documentation process for election systems □ Never leave a systems network with access unattended unless they are in a locked area	

	□ Control physical access to election equipment at all times □ Use tamper evident seals on election equipment, even when they are not in use for elections □ Use functioning conventional or digital lock to protect all entry points to election facilities □ When locking up election equipment, use an access control key or password, have one or more person as a witness and sign a log verifying the equipment is secure □ Monitor entry and exist points to election facilities with cameras that have recording capability □ Adhere to the information retention policy time requirements for keeping logs, documentation and camera footage	
NETWORK AND INFRASTRUCTURE		
Install a Next-Generation Firewall	□ Configure the firewall to control outbound activity and block unauthorized access □ Check for patches and updates monthly	
Segment the Network	□ Use the firewall to create a network section dedicated to election functions and data □ Protect access from the rest of the network, other networks and the Internet □ Restrict access to the election segment of the network to only election employees	
Update Unsupported Operations Systems and Software	□ Upgrade or replace operating systems earlier than Windows 10 Professional or Windows 10 Enterprise	

	□ Ensure all election-related software is current and security patches are up to date □ Check for patches and updates monthly	
Restrict Remote Network Access	□ Limit remote access to the election network □ Tightly control remote access tools and limit use to select employees. □ Vendors must meet the terms of the Vendor Risk Management Policy before connecting to the network □ Prohibit network access through Internet access points not protected by the firewall	
Use Endpoint Security Solutions	□ Ensure Endpoint Security Solutions detect and block threats □ Deploy on all endpoint devices, except systems provided for vote tabulation □ Check for patches and updates monthly	
Implement Software and Network Whitelisting	□ Configure election systems with software that prohibits unapproved software packages □ Establish an approval process for software installation □ Prevent unapproved devices from communicating with systems behind the firewall □ Disable unused network ports at the network switch Ensure active ports block access to unapproved devices	
Secure Wireless Networks and Devices	□ Disable Wi-Fi and Bluetooth wireless devices that are not in use or not defined in the acceptable use policy	□ Create a policy that defines the acceptable use of wireless devices

	□ Segment the network to separate all other Wi-Fi networks from the election department's Wi-Fi network	□ Configure Wi-Fi networks to use WPA2 or later security controls □ Ensure passphrases meet minimum password standards □ Hide the election department SSID □ Restrict polling location wireless networks to required ePollbook functionality only
Backup Data Offsite Using Encryption	□ Backup daily to an encrypted system offsite and not connected to the election network □ Backup all data related to election activities □ Encrypt and store data at FIPS 140-2 encryption levels	
Encrypt Election and Voter Information	□ Encrypt data storage for servers that support elections □ Require encryption for cloud solutions used to store voter registration and critical election information	□ Encrypt hard disks of computer systems that access and process voter registration and critical election data
Manage Removable Media Use	□ Create a Removable Media Policy as required in the Election Information Security Policy template □ Allow only encrypted USB devices for general purpose removable media □ Assign management of election-related removable media devices to one person □ Track removable media assignments in a log and regulate use at all times	□ Use software that controls the use of removable media devices □ Put removable media devices that transfer information between non-connected elections systems through a USB cleaning process □ Delete contents and securely destroy single-use removable media
Track Inventory	□ Create a detailed inventory list of all technology used to support and conduct an election	□ Divide the inventory list into three separate sections: early voting, election day and between elections

	□ Maintain a digital or paper log of approved software and removable media	□ When reusing a device, add a description of device contents to the inventory list before erasing the information □ Keep inventory records for the time specified in the information retention policy.
SUPPORTING TECHNOLOGY		
Protect Email and Website Domains	□ Only use government-provided email addresses and web services using the Internet domain texas.gov or tx.us □ Never perform election business from a non-government email address or website □ Update election website software with critical patches once per month □ Perform penetration tests once per year on election websites	□ Ensure all election website transmissions use a SSL certificate □ Implement a Web Application Firewall
Implement Email Security	□ Disable or require multi-factor authentication for web-based Internet access to email □ Integrate DMARC into your email system	□ Use multifactor authentication to control access all email accounts □ Implement SPAM filtering □ Use anti-virus scanning tools
Password and Multifactor Authentication (MFA)	□ Assign unique usernames to staff members authorized to access any system used for election functions □ Do not allow shared user accounts □ Use a password management solution that uses an encrypted format and requires MFA □ Configure password policies on all systems to require complex passwords □ Require MFA for Domain Administrator access □ Ensure any system accessed remotely to support election processes uses MFA	□ Use MFA on all systems whenever possible □ Use soft tokens as the second user identifying factor instead of text or email □ Discourage staff from sharing passwords or joint accounts □ Change system default passwords immediately after initial new system or device setup

Limit Administrator Access	□ Add constraints for the Local Administrator Account □ Limit access to Domain Administrator accounts to authorized personnel only	□ Establish a user hierarchy based on the Principle of Least Privilege □ Implement an approval process for administrator access □ Ensure that administrators use a user account for routing operations separate from the administrator account used for administrative tasks

APPENDIX C: GLOSSARY

CHECKSUM	A technique used to verify that a file is not corrupted by a virus or other code by using a unique digital fingerprint of the data.
CONTINUITY OF OPERATIONS PLAN	Procedures that enable the election department to continue to operate with minimal disruption during a cyberattack or other disaster.
CYBER THREATS	Criminal activity seeking to undermine elections or steal data for financial gain using the Internet to disrupt or infiltrate election technology
CYBERSECURITY RISKS	Gaps in security practices that present opportunities for cyber criminals to successfully attack election departments.
DENIAL OF SERVICE (DoS)	An attack in which the cybercriminal blocks user access to a computer network.
DOMAIN-BASED MESSAGE AUTHENTICATION REPORTING AND CONFORMANCE (DMARC)	An email validation protocol that protects email domains from unauthorized use.
ELECTION INFORMATION SECURITY POLICY	Protocols that protect election-related data from cyber threats and other disasters.
ELECTION SECURITY ASSESSMENT (ESA)	Cybersecurity reviews to determine the security status of election departments and identify areas for improvement.
ELECTION SYSTEM SECURITY PLAN	Protocols that protect election systems from cyber threats or other disasters.
END-OF-LIFE	The point at which a computer, system, or software should be retired because it can no longer function at optimal levels due to wear, outdated technology, and lack of manufacturer support.
ENDPOINTS	User devices such as computers, laptops, tablets, and printers that are connected to the network.
ENTERPRISE-CLASS SYSTEM	A system with advanced capabilities and large capacity to handle high volume and complex demands.
FEDERAL INFORMATION PROCESSING STANDARD (FIPS) 140-2	A U.S. government computer security standard used to approve cryptographic modules used to encrypt and decrypt data.
HOST INTRUSION DETECTION SYSTEM (HIDS)	A detection system that monitors and analyzes internal computing systems for evidence of attack activity.
INCIDENT CONTAINMENT	Removing infected systems from the network as quickly as possible to stop an attacker's movement through a network and prevent further damage.
INCIDENT RESPONSE PLAN	Procedures for reacting to a cyberattack (referred to as an incident) in ways that minimize the damage and enable the election department to recover as quickly as possible.
INFRASTRUCTURE	All components that enable and secure the network including devices, firewalls, and Internet connectivity.

MALWARE	Software that contains a virus to infect systems allowing attackers to steal or destroy data.
MULTIFACTOR AUTHENTICATION (MFA)	A security control that requires more than one way to verify a user’s identity before allowing login.
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)	A recognized authority on security that establishes standards widely followed in the cybersecurity industry.
NETWORK	The group of devices such as computer systems, printers, tablets, and servers linked together wirelessly and/or with cables.
NETWORK PORT	A number that identifies a connection point in the network.
NETWORK SEGMENTATION	Dividing the network into portions separated from the rest of the network to limit access if an attacker gets into the network and manage traffic flow.
NETWORK SWITCH	Hardware device that directs incoming data from multiple input ports to its intended destination.
NEXT-GENERATION FIREWALL (NGFW)	A system that blocks unauthorized network traffic and offers additional functionality such as inspecting applications and preventing intrusions.
PATCH MANAGEMENT	Adhering to a schedule of checking for software and system updates and installing them to ensure the most current cyberattack protections are in place.
PLAN	A detailed step-by-step process defining how election departments will handle specific situations to achieve objectives.
POLICY	Established protocols related to an objective that define how staff should perform activities and manage resources.
PORT SCAN BLOCKING	Preventing attackers from scanning the network to find open ports they can use to get inside the network.
PRINCIPLE OF LEAST PRIVILEGE	A system, application and data access control practice that limits each user’s access to only the needed levels.
RANSOMWARE	A form of malware in which the attacker demands payment to restore the system and data.
REMEDIATION	Fixing security gaps and improving defenses.
REMOVABLE MEDIA	Storage devices that can be removed from a computer while the system is running such as USB keys or drives, CDs, and DVDs.
SECURE SOCKET LAYER (SSL)	A technology that establishes an encrypted link between a website and a browser.
SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)	Software that collects data generated by systems, security devices and applications that could indicate attack attempts. Security Analysts review the data to determine if a threat is present.
SERVICE SET IDENTIFIER (SSID)	A sequence of characters that uniquely names a wireless local area network (WLAN.)
SOCIAL ENGINEERING	An attack in which a cybercriminal gains access to systems or the network by pretending to be a legitimate voter or citizen to trick an employee into providing usernames and passwords or other access information.
SOFT TOKENS	A software-based multifactor authentication method compared to hard token key FOB or smart card.

STATEFUL DEEP PACKET INSPECTION	A firewall technology that monitors active connections to determine what should be allowed past the firewall.
SYSTEM OR APPLICATION ADMINISTRATOR ACCESS	An account for an application, email or website domain, or system that provides the user with full functionality enabling them to manage other user accounts, enable or block access and make configuration changes.
UTILITIES	Software programs that add functionality to computers or systems.
VENDOR RISK MANAGEMENT POLICY	Protocols that ensure third-party vendors are not introducing security gaps that bad actors can exploit to stage an attack.
VIRTUAL PRIVATE NETWORK (VPN)	An encrypted connection over the Internet that provides secure access for remote computers or devices.
VULNERABILITY SCANNING	An inspection of computers and networks to identify security holes that an attacker could exploit.
WEB APPLICATION FIREWALL (WAF)	Software, a device or service that filters, monitors and blocks malicious traffic from entering a website as well as preventing unauthorized data from leaving a website.
WEB SERVER	A computer system that runs websites. It includes a program that distributes web pages as website visitors click on page web addresses.
WI-FI PROTECTED ACCESS 2 (WPA2)	Security protocol that secures wireless computer networks by using Advanced Encryption Standard (AES), a stronger encryption technology than previous versions.
WRITTEN INFORMATION SECURITY POLICY (WISP)	A set of policies and plans that define how to protect elections from cyberattack and how to respond if an incident occurs. It authorizes employees to quickly perform the described actions without waiting for approval during an attack.

EXAMPLE ELECTION SYSTEM SECURITY PLAN

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

VOTER REGISTRATION SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION
Voter Registration Document File Server	*[Server Model]*	EA0004	IT Server Room	Vendor IT Administrator	Confidential
EA Laptop 1	*[Computer Model]*	EA0001	Elections Department	IT Administrator	Confidential
EA Laptop 2	*[Computer Model]*	EA0002	Elections Department	IT Administrator	Confidential
EA Laptop 3	*[Computer Model]*	EA0003	Elections Department	IT Administrator	Confidential
Firewall	*[Firewall Model]*	IT0027	IT Server Room	IT Administrator	Confidential
Switch	*[Switch Model]*	IT0017	IT Server Room	IT Administrator	Confidential
Router	*[Router Model]*	IT0025	IT Server Room	IT Administrator	Confidential
Windows DC	*[Server Model]*	IT0018	IT Server Room	IT Administrator	Confidential
TEAM			Internet	Elections Administrator	Confidential

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

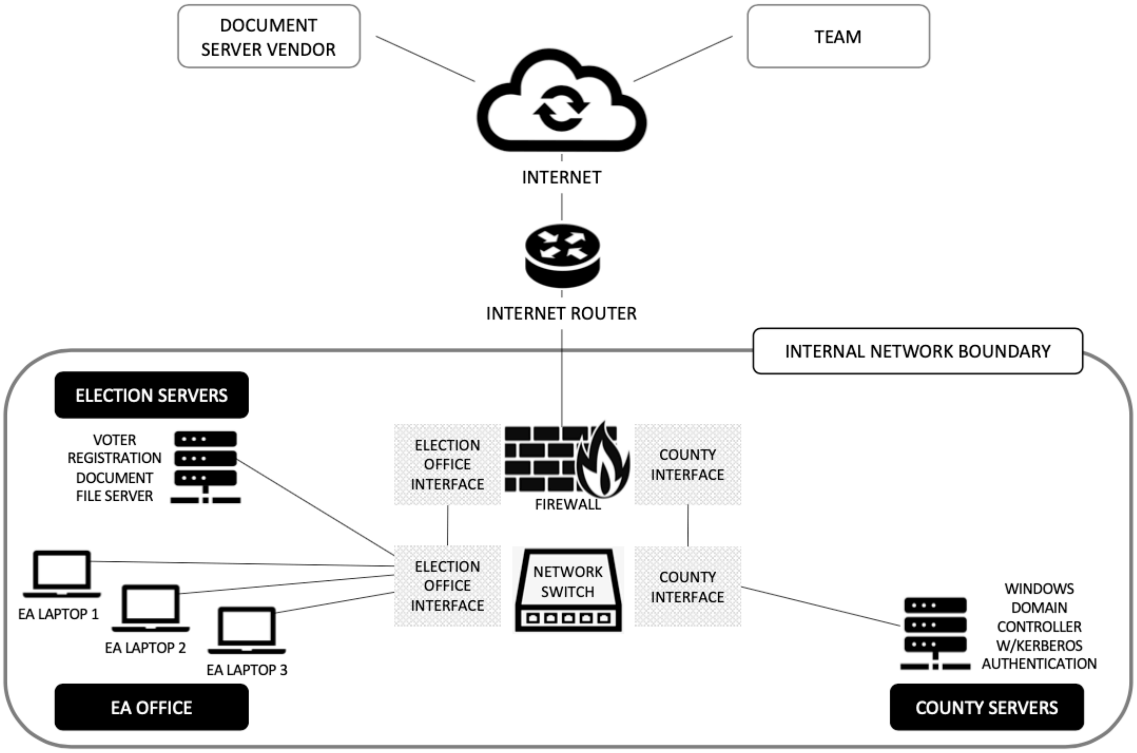
VOTER REGISTRATION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED
TEAM Elections–VR–Senior Role (Full Access)	Internal	P	• Maintain/coordinate county user information with SOS • Maintain county voter registration records • Maintain list of county voters • Oversee all county list maintenance activities	• Voter Registration • Election Administration
TEAM Elections–VR–Deputy/Clerk (Limited Access)	Internal	G	• Input/update county voter registration records • Assist with county list maintenance activities	• Voter Registration • Election Administration • FPCA/Absentee Clerk • VR Clerk
TEAM Elections–VR–Temporary (View Only)	Internal	G	• Research county voter registration records (View only)	• VR Temp
County–User	Internal	G	• Change or remove password • Change user account picture • Change theme and desktop settings • View files stored in user's personal folders and in public folders	• Email • Microsoft Office • FileShare access • Scan Voter Registration documents

VOTER REGISTRATION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED
IT-Administrator-EA	Internal	P	• Create, change, and delete accounts. • Change settings that affect all of the computer's users. • Change security-related settings. • Install and remove apps. • Access system files and files in other user account profiles	• Manages computers and network equipment
Document-Server-Administrator	External	P	• Create, change, and delete accounts • Change settings that affect all of the computer's users • Change security-related settings • Install and remove apps • Access system files and files in other user account profiles	• Manages the Voter Registration document server

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

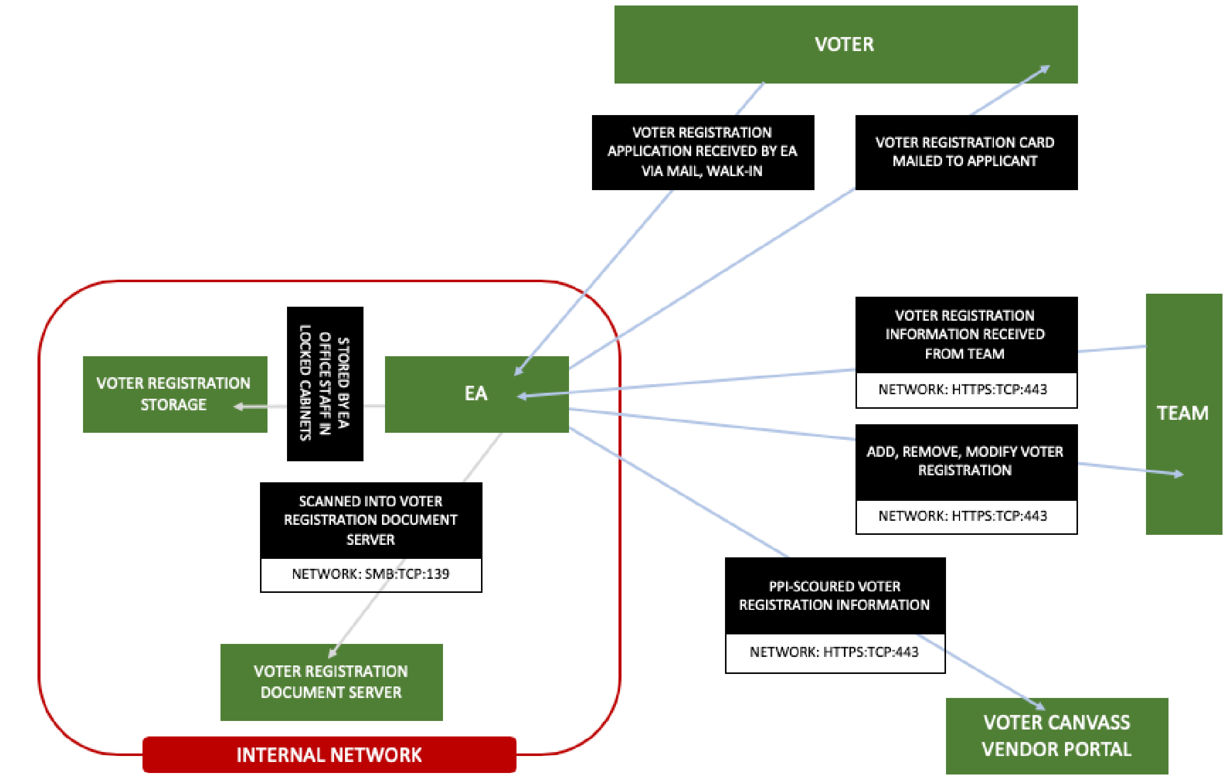
In the space that follows, insert a network architecture diagram for your election management system. Major security components should be represented, including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.



Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across your election management system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.


VOTER
VOTER REGISTRATION APPLICATION RECEIVED BY EA VIA MAIL, WALK-IN
VOTER REGISTRATION CARD MAILED TO APPLICANT
VOTER REGISTRATION STORAGE
STORED BY EA OFFICE STAFF IN LOCKED CABINETS
EA
VOTER REGISTRATION INFORMATION RECEIVED FROM TEAM
NETWORK: HTTPS:TCP:443
TEAM
ADD, REMOVE, MODIFY VOTER REGISTRATION
NETWORK: HTTPS:TCP:443
SCANNED INTO VOTER REGISTRATION DOCUMENT SERVER
NETWORK: SMB:TCP:139
PPI-SCOURED VOTER REGISTRATION INFORMATION
NETWORK: HTTPS:TCP:443
VOTER REGISTRATION DOCUMENT SERVER
VOTER CANVASS VENDOR PORTAL
INTERNAL NETWORK

Internal network protections include:

- Guests must wear badges and be escorted by an employee.
- All employees must wear badges.
- Full zone coverage using monitored surveillance cameras
- Badge scanners used for access into all offices and storage rooms
- All data is encrypted at rest using *[Strong Encryption]* encryption
- Data in transit is encrypted using TLS encryption
- Access to TEAM uses multi-factor authentication
- Employee access regulated using role-based security and principle of least privilege

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table.

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management	• All employees and guests must wear badges. • Monitored surveillance is occurring • Badge scanners are used where appropriate	Election Administrator	• Access to storage rooms and election areas is limited to authorized individuals with badges • Cameras are set up at all building entrances and exits and monitored by Sheriff's Department • Badge scanners used to access IT equipment and Election Office	Fully implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control	• Users are authorized using Kerberos authentication • Unsuccessful logon attempts are monitored for unauthorized access attempts	IT Director	• Access is limited to authorized users by login assigned and maintained in Active Directory • Unauthorized access attempts are not currently being monitored	Partially implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control	• Data access and authorization is controlled incorporating principal of least privilege	Election Administrator	• County employee access rights to TEAM are reviewed after every election • User access control and permissions are set using role-based group policies • Access reviews are performed semi-annually; all exceptions must be removed within ten business days	Fully implemented
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control	• Digital access to Voter Registration information requires using multi-factor authentication • Manage all network devices using multi-factor authentication	Election Administrator	• Multi-factor authentication is used to authenticate to TEAM • Only single-factor authentication is used to authenticate to Microsoft Active Directory account that accesses digital records on network file share • Only single factor authentication is used to authenticate to network devices.	Partially implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology	• Enable firewall filtering between VLANs • Disable all workstation-to-workstation communication • Create a separate wireless network for personal or untrusted devices	IT Director	• All communications between departments must go through firewall • Currently no group policy is in place to disable workstation-to-workstation communication • Guest network is used for untrusted wireless devices	Partially implemented
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management	• Whitelist applications and software for authorized use • Enforce detailed audit logging for access to sensitive data or changes to sensitive data • Maintain separate environments for production and non-production systems	IT Director	• Current software inventory management software does not allow for application whitelisting • No log management currently occurring • All systems and software currently being updated without an internal review	Not currently implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection	• Data-at-rest encryption is used on all servers • Data-at-rest encryption is used on all laptops and removable media	IT Director	• Data on laptop systems is encrypted with *[strong encryption]* encryption • Servers are encrypted with *[strong encryption]* encryption • Removable media, such as USBs is not yet encrypted	Partially implemented
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection	• All sensitive information encrypted in transit	IT Director	• Wireless data is encrypted using *[strong encryption]* encryption • All credentials are transmitted using encryption • HTTPS using TLS is forced on *[Browser].* • *[Encryption Software]* is used for email encryption	Fully implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection	• All system data is automatically backed up on a regular basis • Backups are encrypted • Regular testing of data integrity on backups	IT Director	• All backups are scheduled and done using *[Backup Software]* • Backups are encrypted in transit and at rest using *[strong encryption]* encryption • Weekly schedule is maintained for backup testing with procedures and checklist. The sign-off sheet is audited periodically.	Fully implemented
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection	• All backups have at least one backup destination that is not continuously on the network	IT Director	• No backups are currently being sent offsite or detached from the network	Not currently implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance	• Incorporate patch management • Conduct periodic network scans to find vulnerable systems and software • Utilize risk-rating process for remediation or acceptance of discovered vulnerabilities	IT Director	• *[Software Manager]* is used to manage and update software and hardware patches, including third-party software • *[Vulnerability Scanning Software]* is used to scan for vulnerabilities • Currently no vulnerability management program for addressing and accepting discovered vulnerabilities	Partially implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance	• Maintenance and repair of organizational assets logged and performed with approved and controlled tools. • Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	IT Director	• *[Maintenance Software]* is used to log and update maintenance requests. • Remote maintenance is done using *[Remote Maintenance Software]*and must be approved by asset owner prior to commencement • Details of maintenance must be logged, and temporary access is granted only to assets, as necessary • All sessions are monitored and can be audited.	Fully implemented

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring	• Local logging has been enabled on all systems and networking devices. • All logs are being aggregated to a central log management system for analysis and review. • Log reviewed regularly to identify anomalies or abnormal events.	IT Director	• All computer logs are turned on by group policy. All network device logs are turned on by default. • Logs are not centrally aggregated • Logs are reviewed only when an incident occurs	Partially implemented

HOW TO USE THIS TEMPLATE

This template will function as your Election System Security Plan once you have added the information that is specific to your election department. It provides clear instructions for handling a cyberattack so employees, community leaders, and other stakeholders can block threat activity, minimize the damage, and begin the recovery process as quickly as possible. You, the Election Authority should revise this plan to make it relevant to your staff, vendors, your office environment and voting facilities, your resources, and your election processes.

In the Election Security Best Practices Guide provided in the Texas Election Security Toolkit, the Texas Secretary of State (SOS) prescribes the creation of an Election Written Information Security Program (WISP). An Election WISP is a set of five documents establishing policies that protect elections from cyber threats as well as plans that keep elections running in the event of a cyberattack or disruption.

Documents that comprise the Written Information Security Policy (WISP):

1. Election Information Security Policy
2. Election Incident Response Plan
3. Continuity of Operations Plan
4. Election System Security
5. Vendor Risk Management Policy

IMPORTANT THINGS TO KNOW ABOUT THIS DOCUMENT

- This document provides a Plan that defines how the objectives and requirements established by the Election Information Security Policy will be implemented and achieved for the major systems used for election management and operations. The plan created is expected to be authorized by your County and used for many years with regular reviews and updates, even as your staff and County continue to change.
- Once it is completed and authorized, this document will serve as **Your Plan** that you must adopt and adapt to the needs of **Your County**. SOS provides this template as a starting place, but you are expected to review and make changes, as appropriate for your County. **You, the County Election Authority Leadership are ultimately responsible for the security of your election**.
- Many of the actions and considerations defined in this plan will apply to most Election Authorities. Depending on the needs of your organization, your plan may have additional guidelines, or it may not have as many.
- Some of the election system security options may not apply to you because of variations in facilities, organizational structure, and other factors, but you, the Election Authority must establish and adopt all of the elements in this plan that are relevant to your organization.
- This plan template must be reviewed and updated before being adopted by your county.
- Some sections of the plan will require you provide the details specific to your organization. These areas are pre-filled with suggestions or examples marked with underlined and italicized text.

- You are encouraged to add your own specific plan instructions if you wish to clarify or prescribe election system security actions for purposes that are unique to your environment.
- Securing election systems is an ongoing process. This plan provides you with a formal and documented way to track the progress of implementing security measures that address the risks and threats that elections may face.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR PLAN

1. Read through the entire plan template without making any changes, so you understand its full scope.
2. Read through the plan template again, this time marking each instruction as belonging to one of the following categories:
    - **Yes**
      Applies to you and no revisions are needed
    - **Yes +**
      Applies to you, but needs to be refined with simple known revisions that make it relevant
    - **Maybe**
      Applies to you, but needs additional information that is not yet known or decisions that can only be made by someone else or a group of people
    - **No**
      Does not apply to you because the action references a process or resource that is not needed by your organization
3. Start working on adapting the plan to your specific criteria by making the needed revisions to the "Yes +" category.
4. Delete the actions that fall into the "No" category.
5. Gather the information needed for the "Maybe" category and obtain the needed decisions.
    - Delete an action or procedure if a decision deems it no longer applicable to you and puts it in the "No" category.
    - Add decisions to your plan that fall into the "Yes" category.
6. Replace the underlined, italicized suggestions with your own details.
7. Make copies of the forms and store them with the printed version of the Election WISP where staff can access and use them in the event of a cyberattack.

After you tailor the document to your election organization, it will become your Election System Security Plan and a part of your Election WISP. Follow the storage and document management processes for this document and the rest of the Election WISP as defined in your Election Information Security Policy.

ASSISTANCE FROM TEXAS SOS ELECTION SECURITY TRAINERS

If you have questions or need help customizing this Election System Security Plan to your election organization and processes, contact the Texas Secretary of State Office at electionsecurity@sos.texas.gov to request assistance from an election security trainer.

DOCUMENT MANAGEMENT

The Election System Security Plan must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements. It should also be reviewed as new cyberthreats emerge, or when new vendors or organizational changes require plan updates between yearly reviews.

Maintain a record of all plan reviews in the Plan Review Log to validate that the Election System Security Plan is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

PLAN REVIEW LOG

PLAN ADOPTED DATE <Date>				
Drafted By	<Name, Title>	Signature	<Signature>	<Date>
Approved By	<Name, Title>	Signature	<Signature>	<Date>

REVIEW AND REVISION LOG						
REVIEW SCHEDULE:	General Election Years: December after elections Legislative Session Years: July after SOS Law Conference					
Review Date	If Revised, Revision Date	Revision Description (Or Specify “No Revisions” If None Made)	Drafted By: Name, Title	Signature, Date	Approved By: Name, Title	Signature, Date

[ELECTION AUTHORITY NAME]

ELECTION SYSTEM SECURITY PLAN

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *[Election Authority Name]* that is classified as Confidential. Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.

The following types of confidential information may be contained in this Policy:

System names and purposes

Security device configuration information

Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is *[Election Authority Name]* Confidential, and cannot be reproduced or redistributed in any way, shape or form without prior written consent from *[Election Authority Name].*

TABLE OF CONTENTS

ELECTION SYSTEM SECURITY PLAN

Introduction

The Election System Security Plan[1] provides an overview of the functions, components, and cybersecurity requirements for the information systems used to manage elections and enable voting. The plan is used to document a structured process for planning adequate and required security protections and risk management for core and supporting systems for elections.

The *[Election Administrator]* is responsible for ensuring that the plan is prepared, implemented, and monitored for effectiveness. The plan:

- Provides the *[Election Administrator]* and information technology personnel with a blueprint that defines the election system and the security requirements for using and interacting with it
- Describes responsibilities and expected behavior of all individuals who manage, maintain, and perform functions that ensure the security of the election system
- Describes the current and planned controls that provide a level of security that is appropriate for the information that the system transmits, processes, or stores
- A system is composed of computers and technology resources that are grouped together to accomplish a business function. Following this definition, the plan includes the following business functions:
    - Voter Registration
    - ePollbook and Voter Check-in and Qualification System
    - Election Management
    - Ballot Creation and Distribution
    - Vote Casting and Capture
    - Vote Tabulation
    - Election Night Reporting

The Election System Security Plan is needed to adhere to the first policy standard in Policy 1 of your Election Information Security Policy (EISP). Each section in this plan discusses which policies in your EISP it specifically references and which requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) it helps to meet.

[1] NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Federal Information Systems, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

1. ELECTION MANAGEMENT SYSTEM

Purpose

The purpose of the election management system is to provide a resource for planning and organizing the events that are part of the election process. The system provides detailed steps for the preparation of elections that include gathering the candidate and entity issues that will make up the ballot; assembling the polling place staff—from election judges and alternates to poll workers—and paying them as necessary; and tracking the execution of the election process.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

ELECTION MANAGEMENT SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

ELECTION MANAGEMENT SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architecture diagram for your election management system. Major security components should be represented, including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across your election management system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table.

ELECTION MANAGEMENT SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

ELECTION MANAGEMENT SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

ELECTION MANAGEMENT SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

ELECTION MANAGEMENT SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

ELECTION MANAGEMENT SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

2. VOTER REGISTRATION SYSTEM

Purpose

The purpose of the voter registration system is to manage the registration of voters within the County. The system allows the County to add, remove, and transfer voters who register to vote in the County as well as coordinate registered voters within the State of Texas between County Registrars. The system also keeps track of actions that take place in a voter's registration record, such as voter history, address confidentiality, and ballot-by-mail activity.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

VOTER REGISTRATION SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

VOTER REGISTRATION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In in the space that follows, insert a network architecture diagram for your voter registration system. Major security components should be represented including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

VOTER REGISTRATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

3. EPOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM

Purpose

The purpose of the ePollbook/voter check-in and qualification system is to enable qualification of voters at the polling place and to provide each voter with the correct ballot style based on his or her registered precinct. The system allows the County to notate voters' records as they vote in person or are sent a ballot by mail. These sections ensure that voters cannot vote multiple times in one election and provide voting history updates during and after the election.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architecture diagram. Major security components should be represented including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

ePOLLBOOK AND VOTER CHECK-IN AND QUALIFICATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

4. BALLOT CREATION AND DISTRIBUTION SYSTEM

Purpose

The purpose of the ballot creation and distribution system is to design the ballot, incorporating various ballot styles to ensure that voter intent can be accurately determined. Ballot creation can include the layout of paper ballots or the programming of an election into the election management system to configure ballot capture systems such as direct-recording electronic (DRE) equipment, Ballot Marking Devices (BMDs) and ballot scanners. Ballot distribution involves moving ballots from the election facility to the polling places and back to the election facility. It includes electronic voting devices, paper ballots, and alternative ballots including provisional ballots and remote voting for deployed military members.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

BALLOT CREATION AND DISTRIBUTION SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

BALLOT CREATION AND DISTRIBUTION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architectural diagram. Major security components should be represented including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5

- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

BALLOT CREATION AND DISTRIBUTION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

BALLOT CREATION AND DISTRIBUTION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

BALLOT CREATION AND DISTRIBUTION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

BALLOT CREATION AND DISTRIBUTION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

BALLOT CREATION AND DISTRIBUTION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

5. VOTE CASTING AND CAPTURE SYSTEM

Purpose

The purpose of the vote casting and capture system is to facilitate voters casting their ballots and to record voters' choices accurately and securely. This system includes the return of ballots to the tabulation area—both electronic and paper form ballots—and encompasses early voting, ballot by mail, and Election Day voting.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

VOTE CASTING AND CAPTURE SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

VOTE CASTING AND CAPTURE SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architecture diagram. Major security components should be represented including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

VOTE CASTING AND CAPTURE SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

VOTE CASTING AND CAPTURE SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

VOTE CASTING AND CAPTURE SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

VOTE CASTING AND CAPTURE SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

VOTE CASTING AND CAPTURE SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

6. VOTE TABULATION SYSTEM

Purpose

The purpose of the vote tabulation system is to count votes and determine the results for each race and proposition that appeared on the ballot. Results must be able to be reported both collectively and on a precinct-by-precinct basis. The system produces results that are used to compare the number of voters who received ballots to the number of ballots cast.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

VOTE TABULATION SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

VOTE TABULATION SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architectural diagram. Major security components should be represented including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across your election management system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

VOTE TABULATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

VOTE TABULATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

VOTE TABULATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

VOTE TABULATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

VOTE TABULATION SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

7. ELECTION NIGHT REPORTING SYSTEM

Purpose

The purpose of the election night reporting system is to distribute results to the public and report the election results to the Secretary of State. The election night reporting system can include not only the State's system but also the County's official website. Unofficial and official results should only be published to the Secretary of State's website and the County's official website. Social media and other communications should only refer the public to these sites for results.

Component Inventory

- Adheres to the following EISP security standards: Policy 5; Policy 6
- Meets the following requirements of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF): ID.AM-1, ID.AM-2, ID.AM-5, ID.AM-6, ID.BE-4

ELECTION NIGHT REPORTING SYSTEM					
DEVICE NAME	DEVICE MODEL	ASSET TAG	LOCATION	SYSTEM ADMINISTRATOR	DATA CLASSIFICATION

Authorized Users, Roles, and Permissions

- Adheres to the following EISP security standards: Policy 7
- Meets the following requirements of the NIST CSF: ID.AM-6, PR.AC-4, PR.AT-2, ID.RA-3, ID.GV-2

ELECTION NIGHT REPORTING SYSTEM				
ROLE	INTERNAL OR EXTERNAL	PRIVILEGED (P), OR GENERAL (G) USER	AUTHORIZED PRIVILEGES	FUNCTIONS PERFORMED

Network Architecture

- Adheres to the following EISP security standards: Policy 8
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-4

In the space that follows, insert a network architecture diagram. Major security components should be represented, including hostnames, authentication and access controls, firewalls and network devices, database servers, major applications, storage, and internet connectivity.

Data Flow

- Adheres to the following EISP security standards: Policy 5
- Meets the following requirements of the NIST CSF: ID.AM-3, ID.AM-5

In the space that follows, insert a data flow diagram and describe the flow of data across your election management system boundaries, both into and out of the system. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users.

Protections and Controls

- Adheres to the following EISP security standards: Policy 5; Policy 6; Policy 7; Policy 8; Policy 9; Policy 11
- NIST CSF requirements are mapped in the table

ELECTION NIGHT REPORTING SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Physical Protections (Access and Environment)	PR.AC.2: Physical access to assets is managed and protected	Policy 5: Asset Management			•	
User Access and Authentication	PR.AC-1: Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes; PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				

ELECTION NIGHT REPORTING SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Roles and Authorizations	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	Policy 7: Identity Management, Authentication, and Access Control				
Multi-Factor Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor authentication) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	Policy 7: Identity Management, Authentication, and Access Control				
Network and Internet Protections	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	Policy 9: Use of Protective Technology				

ELECTION NIGHT REPORTING SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Integrity Protections and Validations	PR.DS-6: Integrity-checking mechanisms are used to verify software, firmware, and information integrity; PR.DS-7: The development and testing environment(s) are separate from the production environment	Policy 5: Asset Management				
Data-at-Rest Protections (encryption)	PR.DS-1: Data-at-rest is protected	Policy 6: Data Security and Information Protection				
Data-in-Transit Protections (encryption)	PR.DS-2: Data-in-transit is protected	Policy 6: Data Security and Information Protection				
Data Backup and Recovery	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	Policy 6: Data Security and Information Protection				

ELECTION NIGHT REPORTING SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
System Redundancy, Resiliency and Recovery	PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	Policy 6: Data Security and Information Protection				
Vulnerability Management	PR.IP-12: A vulnerability management plan is developed and implemented	Policy 8: Election Information System Maintenance				

ELECTION NIGHT REPORTING SYSTEM						
CONTROL	NIST CSF	POLICY	CONTROL DESCRIPTION	CONTROL OWNER	IMPLEMENTATION DESCRIPTION	IMPLEMENTATION STATUS
Maintenance and Remote Maintenance Security	PR.MA-1: Maintenance and repair of organizational assets is performed and logged, with approved and controlled tools; PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	Policy 8: Election Information System Maintenance				
Audit trail and event logging	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	Policy 11: Continuous Security Monitoring				

HOW TO USE THIS INCIDENT RESPONSE PLAN TEMPLATE

This template is intended to become your Election Incident Response Plan once you have added the information specific to your election department. It provides clear instructions for handling a cyberattack so employees, community leaders and other stakeholders can block threat activity, minimize the damage and begin the recovery process as quickly as possible. Election Authorities should revise this plan to make it relevant to your staff, vendors, your office environment and voting facilities, your resources and your election processes.

In the Election Security Best Practices Guide provided in the Texas Election Security Toolkit, the Texas Secretary of State (SOS) prescribes the creation of an Election Written Information Security Program (WISP). An Election WISP is a set of five documents establishing policies that protect elections from cyber threats as well as plans that keep elections running in the event of a cyberattack or disruption.

1. Election Information Security Policy
2. Election Incident Response Plan
3. Election Continuity of Operations Plan
4. Election System Security
5. Election Vendor Risk Management Policy

A technical Election Incident Response Plan is available upon request from electionsecurity@sos.texas.gov. It details how the sections in this document align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a widely accepted standard for security.

IMPORTANT THINGS TO KNOW ABOUT THIS DOCUMENT

- This document provides a **Plan** that defines the actions you will take as soon as an incident is detected and confirmed. The plan is expected to be authorized by your county and used for many years with regular reviews and updates, even as your staff and county continues to change.
- When completed, this document defines **Your Plan** that you must adopt and institute in **Your County**. SOS provides this template as a starting place, but you are expected to review and change it, as appropriate for your County. **County Election Authority Leadership is ultimately responsible for the security of your election.**
    - Many of the actions defined in this plan will apply to most Election Authorities. You may wind up with a plan that excludes some of the actions in this template, or you may need to add more procedures to cover all of your organization's functions and circumstances.
    - Some of the incident response actions may not apply to you because of variations in facilities, organizational structure and other factors, but your Election Authority should implement all of the elements in this plan that are relevant to your organization.
- This provided template must be reviewed and updated before use.

    - Some sections of the plan will require that you fill in the details specific to your organization. These areas are pre-filled with suggestions or examples marked with underlined and italicized text.
    - You are encouraged to add your own specific actions if you need to clarify or prescribe incident response procedures for purposes that are unique to your environment.
    - The Appendices consist of example logs and forms to use when assigning staff incident response responsibilities and logging or tracking procedures as defined in the plan. These are worksheets are not considered part of the Election Incident Response Plan because they are actively used to facilitate the action steps required when handling an incident.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR PLAN

1. Read the plan in its entirety first without making any changes for the purpose of understanding the full scope of the plan.
2. Read the plan again and mark each action or procedure as belonging to one of the following categories:
    - **Yes**
      Applies to you and no revisions are needed
    - **Yes +**
      Applies to you, but needs to be refined with simple known revisions that make it more relevant
    - **Maybe**
      Applies to you, but needs additional information that is not yet known or decisions that can only be made by someone else or a group of people
    - **No**
      Does not apply to you because the action references a process or resource that is not needed by your organization
3. Start working on adapting the plan to your specific criteria by making the needed revisions to the “Yes +” category.
4. Delete the actions that fall into the “No” category.
5. Gather the information needed for the “Maybe” category and obtain the needed decisions.
    - Delete an action or procedure if a decision deems it no longer applicable to you and puts it in the “No” category.
    - Add decisions to your plan that fall into the “Yes” category.
6. Replace the underlined, italicized suggestions with your own details.
7. Gather and organize the needed resources for the Incident Response Command Center.
8. Create the contact lists and other written documents required throughout the plan.
9. Make copies of the logs and forms in the Appendices and store the copies with the printed version of the Election WISP where staff can access and use them in the event of a cyberattack.

After you tailor the document to your election organization, this document is your Election Incident Response Plan and a part of your Election WISP. Follow the storage and document management processes for this document and the rest of the Election WISP as defined in your Election Information Security Policy, which is the first document you received in the Texas Election Security Toolkit.

ASSISTANCE FROM TEXAS SOS ELECTION SECURITY TRAINERS

If you have questions or need help customizing this Election Incident Response Plan to your election organization and processes, contact the Texas Secretary of State Office at electionsecurity@sos.texas.gov to request assistance from an election security trainer.

DOCUMENT MANAGEMENT

The Election Incident Response Plan must be reviewed at least once per year. It must be reviewed and updated more frequently when state or federal legislation mandates new election security requirements, new cyber threats require plan changes or needed improvements emerge from practice incident response drills as part of Table-Top exercises.

Maintain a record of all plan reviews in the Plan Review Log to validate that the Election Incident Response Plan is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

PLAN REVIEW LOG

ORIGINAL EFFECTIVE DATE <Date>						
Drafted By		<Name, Title>		Signature	<Signature>	<Date>
Approved By		<Name, Title>		Signature	<Signature>	<Date>
REVIEW AND REVISION LOG						
REVIEW SCHEDULE		General Election Years: December after elections		Legislative Session Years: July after SOS Law Conference		After an incident or practice drill
Review Date	Revision Date	Revision Description	Drafted By: Name, Title	Signature, Date	Approved By: Name, Title	Signature, Date

ELECTION AUTHORITY NAME

ELECTION INCIDENT

RESPONSE PLAN

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *Election Authority Name* that is classified as Confidential. Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.

The following types of confidential information may be contained in this Policy:
System names and purposes
Security device configuration information
Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is *Election Authority Name* Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *Election Authority Name*.

Contents

ELECTION INCIDENT RESPONSE PLAN

[*Election Authority Name*] must follow these steps to respond to a security incident:

STEP 1: DETERMINE IF THE EVENT IS A CONFIRMED SECURITY INCIDENT

- Suspected cyber incidents must be immediately reported to the [*Election Administrator or Designee*] who is authorized to take the lead as the Incident Response Commander as defined in the Incident Response Team Roles and Responsibilities Chart (SEE APPENDIX C)
- The Incident Response Commander must submit the details of a possible cyber incident to [specify a role or entity that has the knowledge to decide if an attack has happened such as a staff member with cybersecurity training, IT staff member, IT or security vendor, or Texas Department of Information Resources (DIR)] to confirm validity before it is declared an incident. Potential attack methods should be considered when determining if an incident has occurred including:
    - Viruses from external/removable media
    - Email that triggered malware or ransomware
    - Email phishing campaigns that exposed access credentials resulting in a breach
    - Access to credential theft through hacking
    - Device, system or equipment tampering
    - Loss or theft of equipment
- If there is doubt about the validity of a possible incident, escalate the issue to [*specify a role or entity with in-depth cybersecurity expertise such as an IT leader, IT or security vendor leadership or TX DIR*] to conduct a deeper analysis including, but not limited to looking for:
    - Changes in User IDs, Groups, Access Rights
    - File Modification Dates and Ownership
    - Network Configuration Changes and Unusual Activity
    - Unauthorized Applications Running
    - System Binaries
    - Altered Registry Keys
    - Unusual or Hidden Files
    - Modifications to Data or Configuration Files
    - Recent Changes, Failures, Errors, Status Changes, Access/admin Events
    - Access to credentials through hacking or social engineering

STEP 2: BEGIN DOCUMENTING THE RESPONSE

- If the event is determined to be a security incident, the Incident Response Commander must immediately begin tracking response activities in an Incident Handler's Log and Report that will be submitted to the Texas Secretary of State's Office after the incident is remediated. (SEE APPENDIX A).
- Incident Handlers are the individuals on the Incident Response Team (see Notify and Assemble the Incident Response Team in Step 4) who coordinate and execute the efforts to contain the incident, minimize the damage, and begin recovery.
- The Incident Response Commander must record facts, theories and rumors in the Incident Handler's Log and Report to minimize the potential for making misguided decisions or communicating false information.

STEP 3: NOTIFY LEADERSHIP STAKEHOLDERS

- The [*Election Administrator*] must notify all critical stakeholders (only inform those who need to know) at this phase of the response process. Refer to the contact information listed in the Incident Notification Priority Contact List (SEE APPENDIX B).
    - Texas Secretary of State (SOS)
    - Texas Department of Information Resources (DIR)
    - Cybersecurity Service Provider
    - Law Enforcement
    - Legal Counsel
    - Government Officials

STEP 4: NOTIFY AND ASSEMBLE THE INCIDENT RESPONSE TEAM

- The [*Election Administrator*] should immediately contact and gather the Incident Response Team, a cross-functional team composed of organization's stakeholders and Incident Handlers, the individuals pre-assigned to perform incident response tasks as defined in the Incident Response Team Roles and Responsibilities chart. (SEE APPENDIX C)
- As soon as the Incident Response Team is notified, each person identified as an Incident Handler must receive an Incident Handler's Log and Report template (SEE APPENDIX A) to begin recording his or her activities and observations.
- Incident Handlers will submit their completed Incident Handler's Logs and Reports to the Incident Response Commander who will compile them into the master Incident Report at the conclusion of the incident.

STEP 5: ANALYZE THE EVENT FOR SCOPE AND START REPORT

- [*Specify the role or entity that has the knowledge to analyze the incident such as a staff member with cybersecurity training, IT staff member, IT or security vendor, or TX DIR*]. must analyze the incident to confirm the full scope and document the discovered facts in the Incident Handler's Log (SEE APPENDIX A):
    - Source of the issue (outside actor, insider)
    - Motive (Malicious or accidental)
    - List of affected or involved resources (network, systems, data, software, credentials, business processes)
    - The type of data that is involved (sensitive, confidential or other) and what is the quantity of data
    - People affected by the issue (number of people, internal or external, departments)
    - The type of incident:
        - Ransomware
        - Malware
        - Denial of Service
        - Malicious Code
        - Improper Usage
        - Scans/Unauthorized Access
        - Phishing
- [*The Election Administrator*] should determine the severity of the incident as defined in the Incident Severity Classification System in Table 1.

TABLE 1: INCIDENT SEVERITY CLASSIFICATION SYSTEM

SEVERITY CLASSIFICATION	VOTERS AFFECTED	# OF DEPARTMENT USERS IMPACTED	IMPORTANT INDIVIDUALS IMPACTED	APPLICATIONS & SYSTEMS CRITICAL TO OPERATIONS	NON-CRITICAL APPLICATIONS & SYSTEMS
CRITICAL 🔴	Greater Than 50%	Greater Than 25%	County Judge, Elected Officials, Election Administrator	Unavailable, Infiltrated or Data Loss Suspected	Infiltrated or Data Loss Suspected

HIGH 🟠	25% To 50%	15% To 25%	Department Heads, County Officials	Impaired but Available	Unavailable
MODERATE 🟡	10% To 25%	10% To 15%	-	Issues Experienced	Impaired but Available
LOW 🟢	Less Than 10%	Less Than 10%	-	-	Issues Experienced

STEP 6: SET UP A COMMAND CENTER

- The [*Election Administrator and Incident Response Team*] must set up an Incident Response Command Center in the [*Specify a room that can be locked*]. Access to the room should be controlled by keeping the door locked and providing keys to the Incident Response Team only. If electronic access can be granted to the Response Command Center, make sure that only those staff involved in the response have badge controlled access to the room.

STEP 7: ASSEMBLE INCIDENT RESPONSE RESOURCES

- The [*Election Administrator and Incident Response Team]* must gather the resources needed to conduct Incident Response operations in the Command Center as specified in the Incident Response Resource List in Table 2.

TABLE 2: INCIDENT RESPONSE RESOURCE LIST

1. Printed copy of the Election Written Information Security Program (WISP). The printed version of the Election WISP is located [*the location of the printed version of the Election WISP.*] These documents should be placed in a central location in the Incident Response Command Center to remain easily accessible to the Incident Response Team for quick reference.
    - Election Incident Response Plan
    - Election Information Security Policy
        - Asset Inventory
        - Topology Diagram of the Network
        - Data Inventory

   - Continuity of Operations Plan

2. 10 printed copies of the Incident Handler’s Log and Report (APPENDIX A). The copies are stored with printed version of the Election WISP located *[the location of the printed version of the Election WISP].*
3. Instructions for specific technical activities
   - How to run AV scanning
   - How to capture network packets
   - How to restore data from backups
4. White boards and/or projection equipment to provide visibility of Incident Response activity and progress to the team
5. Printed Emergency Contact List of personnel and vendors with names, titles, mobile numbers and email addresses (APPENDIX D). The copies are stored with the printed version of the Election WISP located *[the location of the printed version of the Election WISP].*
6. Spare equipment if primary hardware is quarantined due to the attack
   - Cell phones for alternative communications
   - Three laptops, tablets or other non-affected devices
   - One server, if applicable
   - Cables
   - Basic Networking Equipment – switches, modems, routers etc.
   - Toolkit with all relevant parts and tools necessary to effect repairs
7. Blank USB Drives
8. Blank backup storage units with encryption capabilities
9. Digital backup devices (e.g. hard disk cloners) and software to create disk images, capture memory state of hosts, preserve log files, and save other relevant incident data
10. 10 printed copies of Communication Plan Forms (APPENDIX E)
11. Evidence gathering accessories
    - Hardbound notebooks
    - Digital cameras
    - Audio recorders
    - Evidence / Chain of Custody Log (APPENDIX F)

- Evidence storage bags/tags/tape to preserve evidence for possible legal actions or insurance requirements

12. Written statement listing the circumstances under which the Election Authority will or will not pay a ransom in the event of a ransomware attack. When making this plan, you must consult the entity within your county or city who controls the budget under which you operate.

STEP 8: INITIATE THE CONTINUITY OF OPERATIONS PLAN

- Refer to the Continuity of Operations Plan (COOP) in the Election WISP

STEP 9: WORK WITH THE IT STAFF TO CONTAIN THE DAMAGE

- Possible incident containment activities include, but are not limited to:
  - Disconnect infected devices and systems from the network
  - Segregate affected systems
  - Reroute network traffic to avoid possible infection from the network
  - Filter or block the attack
  - Refer to the Election Authority's written statement regarding the pre-determined response to handling ransomware demands.
  - Continue to investigate scope and additional infected systems and devices
  - Update scanning software to include the virus signature and scan all other devices for possible infection
  - Change passwords for compromised credentials
  - Erase infected drives and remove the virus, malicious code, hacker tools and inappropriate material
  - Preserve and collect all evidence for insurance or law enforcement investigation and maintain an Evidence / Chain of Custody Log (APPENDIX F)

STEP 10: NOTIFY THE INSURANCE PROVIDER, IF APPLICABLE

- *[Election Administrator]* should contact the contracted Cybersecurity Insurance Provider, if applicable, when a cybersecurity incident is confirmed and coordinate with the company to provide the necessary information, documentation and approvals.
- The Cybersecurity Insurance Policy provides coverage for:
  - Breach Costs (including Computer Forensics, Notification, Call Center, Identity Protection Services, Crisis Management and Public Relations)

  - Penalties (includes all amounts awarded in a Regulatory Proceeding)
  - PCI Fines and Assessments
  - Cyber Extortion Costs
  - Business Interruption Costs
  - Data Recovery Costs

INSURANCE PROVIDER	
CARRIER NAME	
POLICY NUMBER	
PRIMARY CONTACT NUMBER	
INCIDENT HOTLINE NUMBER	
AUTHORIZED COUNTY CONTACT	
SECONDARY AUTHORIZED COUNTY CONTACT	

STEP 11: INITIATE THE INTERNAL COMMUNICATIONS PLAN

- The designated Incident Response Team Communications Director must develop and disseminate information about the incident to the internal staff using the Communications Plan. (APPENDIX E).
- The Incident Response Team must maintain secure communications with employees and other internal stakeholders during an incident, limiting communications regarding the details of the incident on a need-to-know basis.
- Internal communications should consist of:
  - Instructions to internal staff regarding steps to take to protect their devices or repair devices affected by the incident
  - Notification to state government leadership regarding the incident
  - Information to other state and/or federal agencies
- Notification details should include:
  - What happened?
  - When did the incident occur and/or when was it detected?

  - How was it detected?
  - What data was potentially compromised?
  - How much data was compromised?
  - Whose data was compromised?
  - Why the recipient is being notified?
  - What steps were/are being taken?
  - What steps should individuals take?
  - If a service is being offered to affected individuals, how long do they have to enroll?
  - Anticipated next steps, if any
  - Who to contact for additional information (Contact name, number, hours of availability, website, hotline, email address, etc.)
  - Signature (The letter should be signed by an official with responsibility over the compromised data)

STEP 12: INITIATE THE EXTERNAL COMMUNICATIONS PLAN

- The designated Incident Response Team Communications Director must develop and disseminate information about the incident to the external stakeholders in alignment with data security policies associated with the Election Data Classification System.
- External communications should consist of:
  - Announcements to third-party vendors
  - Press release to the media
  - A press briefing if the incident is deemed critical
- Elements of a press release and press briefing should include:
  - What happened
  - Resolution
  - Notification has occurred
  - Who is affected/not affected
  - What specific types of personal information are involved
  - What are the (brief) details of the incident
  - Whether or not evidence indicates data has been misused
  - Expression of regret and steps being taken to prevent similar incidents from happening again
  - Major actions taken
  - Where to go for more information

STEP 13: RECOVER THE ASSETS AND DATA

- The Incident Response Team must work with key IT staff to perform recovery processes. Only personnel with expert technical training should engage in the recovery activities. Recovery activities include but are not limited to:
    - Rebuilding and reimaging the devices and systems from scratch
    - Loading backed-up data to the devices and systems
    - Replacing compromised files with clean versions
    - Scanning for traces of malicious software, hacker tools or code
    - Apply all recent patches
    - Testing the devices and systems before reconnecting to the network

STEP 14: DOCUMENT THE INCIDENT IN A CYBERSECURITY INCIDENT REPORT

- If an incident is detected, create a report using the information gathered in the Incident Handler's Logs (APPENDIX A) that includes:
    - How the incident was detected
    - The scope, severity and impact of the incident
    - How the incident occurred
    - The people and departments affected
    - Who was notified and when
    - The steps taken to contain the incident
    - The incident analysis results
    - Internal and external communication
    - Recovery activities
    - How this incident type can be prevented in the future
    - Lessons Learned

STEP 15: IDENTIFY LESSONS LEARNED AND UPDATE THE PLAN

- Upon closure, review each incident via a "lessons-learned" aka "After Actions Review" meeting and document it in the Incident Handler's Log (SEE APPENDIX A). Shouldn't the lessons learned be documented in a revised version of the Incident Response Plan?
- Lessons learned will be integrated into the Cybersecurity Incident Response Plan to improve responses to a future incident, should one occur.
- Access to "After Actions Review" documentation is restricted to Incident Response Team members unless the team determines the report should be released to other approved individuals.

STEP 16: COLLECT AND SUBMIT EVIDENCE

- All evidence must be gathered including infected technology, information about the incident and the Evidence / Chain of Custody Log (APPENDIX F) and submitted to the insurance company, forensics team or law enforcement agency as required.

APPENDIX A: INCIDENT HANDLER'S LOG AND REPORT

COMMUNICATION CHANNELS	CONFERENCE BRIDGE	MOBILE NUMBERS		

INCIDENT FACTS

Incident Number	
Source (Email, Website, Connected Network)	
Motive (Accidental or Malicious)	
Affected Resources	
Data Type (Confidential, Sensitive)	
# People Affected and Department	
Incident Type (Ransomware, DOS, Phishing, etc.)	
Severity (Critical, High, Medium, Low)	

INCIDENT TIMELINE

	DATE/ TIME
Event Occurrence	
Detection	
Classification	
IR Initiated	
Contained	
Remediated	
Recovered	
After Actions Review	

ACTIVITY LOG

DATE/TIME	

"AFTER ACTIONS REVIEW" NOTES

What went well?

What didn't work well?

		What information was needed sooner?
		What protective measures would help prevent the incident from occurring in the future?
		What detection measures would have alerted you sooner?

APPENDIX B: INCIDENT NOTIFICATION PRIORITY CONTACT LIST

Organization	Name	Title	Phone	Email	When to Contact and Why
Office of the Texas Secretary of State (SOS)	Keith Ingram	Director of Elections	512-463-5650	elections@sos.texas.gov	IMMEDIATELY after a valid incident is confirmed in order to engage in coordinated response
Texas Department of Information Resources (DIR)			512-475-4700	Security-alerts@dir.texas.gov	After valid incident is confirmed for assistance with technical aspects of response
Cybersecurity Service Provider					
Law Enforcement					
Legal Counsel					
Government Officials					
EI ISAC/MS ISAC			1-866-787-4722	soc@cisecurity.org	After incident facts have been collected to share information that helps other agencies guard against similar attacks.

APPENDIX C: INCIDENT RESPONSE TEAM ROLES AND RESPONSIBILITIES			
IR TEAM ROLE		RESPONSIBILITIES	PERSON ASSIGNED
INCIDENT HANDLERS	IT STAFF, IT VENDOR OR CYBERSECURITY VENDOR	• Provide technical expertise as needed • Serve in an on-call, 24/7 capacity in the event of an incident • Provide documentation as requested concerning the technical nature of the incident • Document activities in an Incident Handler’s Log and Report	Name: Title: Phone: Email: Date Assigned:

INCIDENT HANDLER	INCIDENT RESPONSE COMMANDER: *[ELECTION ADMINISTRATOR OR DESIGNEE]*	• Function as the central point of contact and the lead for all incidents • Initiate and coordinate incident response activities Start the Cybersecurity Incident Handler's Log and Report as soon as an incident is confirmed and update the report throughout the incident, documenting the incident response activities, timeline, key decision points and rationale, and progress of the remediation efforts • Coordinate the containment and remediation of the incident with the IT Staff • In conjunction with Legal Counsel, ensure that evidence is appropriately gathered, preserved and the chain of custody is maintained • Coordinate the internal and external communication plans. • After the incident has been remediated, compile copies of the Incident Handlers' Logs from other team members and add relevant information to the master report. Complete the report and submit it to the Texas Secretary of State's Office. • Conduct a "Lessons Learned" review after every incident and update the Cybersecurity Incident Response Plan	Name: Title: Phone: Email: Date Assigned:

INDICENT HANDLER	[*DIRECTOR OF COMMUNICATIONS OR DESIGNEE*]	• Serves as the central source of information • Keep the Incident Response Team consistently informed of important media activities • Develops talking points for leadership and anyone communicating with the public and media • Creates press releases for the media • Briefs the press on relevant incident information in accordance with the Election Data Classification System in the Election Information Security Policy • Documents activities in an Incident Handler's Log and Report	Name: Title: Phone: Email: Date Assigned:
STAFF MEMBERS		• Execute the Continuity of Operations Plan • Participate in "Lessons Learned" discussions	Name: Title: Phone: Email: Date Assigned:
COUNTY AUTHORITY LEADERSHIP: *[COMMISSIONER OR DESIGNEE]*		• Stay informed of the incident response progress and advise regarding the operational impact of containment and recovery decisions • Coordinate requirements and engagement with the cybersecurity insurance provider, if applicable	Name: Title: Phone: Email: Date Assigned:
LEGAL COUNSEL		• Engage and supervise outside counsel when warranted • Report incidents to the relevant insurance broker and/or carrier as necessary	Name: Title: Phone: Email:

	• Assesses the extent of legal steps needed (such as the need to direct the forensic investigation) • Oversees the preservation of evidence, and that the chain of custody is maintained • Advises the Incident Response Team on all legal, regulatory and contractual requirements related to the incident, including any obligation to notify external organizations, clients, business partners, affected individuals or regulatory agencies • Determines public reporting obligations • Provides advice on all communications (both internal and external) related to the incident, including any law enforcement authorities • Provides legal support related to an incident (e.g. prosecution of a suspect, handling of lawsuits arising from an incident, developing contracts or other binding agreements for external services)	Date Assigned:
HUMAN RESOURCES LIAISON	• Ensures that employees understand how to respond to inquiries from external parties and understand the County's confidentiality obligations regarding the incident • Provides advice regarding employee relations • Assists with any disciplinary proceedings as appropriate (e.g. if an employee is suspected of causing an incident)	Name: Title: Phone: Email: Date Assigned:

APPENDIX D: EMERGENCY CONTACT LIST

Name	Title	Phone Number	Email	Department

APPENDIX E: C OMMUNICATIONS PLAN

Audience	Frequency	Method	Purpose of the Communication	Person Responsible for the Communication	Date & Time
IT Team Members					
General Counsel					
Human Resources					
Internal Audit					
Crisis Management Team					
Leadership/Management					
Employees					
Commissioners Court					
Outside Counsel					
Law Enforcement					
Operations					
Other Entities					
Cyber Insurance Carrier					
Regulatory Agencies					

APPENDIX F: EVIDENCE / CHAIN OF CUSTODY FORM

Item #	Quantity	Description of Item (Model, Serial #, Condition, Identifying Marks or Characteristics)

Item #	Date / Time	Released by (Name)	Released by (Signature)	Received by (Name)	Received by (Signature)	Comments / Location

HOW TO USE THIS VENDOR RISK MANAGEMENT POLICY TEMPLATE

This document is the **Vendor Risk Management Policy**. It is presented in the form of an assessment survey that vendors must complete to determine if they follow the security practices and processes that that they are expected to follow in order to protect election information and systems from theft, loss, and manipulation. You, the Election Authority should revise this Policy to make it relevant to your staff, your vendors, your office environment and voting facilities, your resources, and your election processes.

In the Election Security Best Practices Guide provided in the Texas Election Security Toolkit, the Texas Secretary of State (SOS) prescribes the creation of an Election Written Information Security Program (WISP). An Election WISP is a set of five documents establishing policies that protect elections from cyberthreats as well as plans that keep elections running in the event of a cyberattack or disruption. Those documents are listed below.

1. Election Information Security Policy
2. Security Incident Response Plan
3. Continuity of Operations Plan
4. Election System Security Plan
5. Vendor Risk Management Policy

IMPORTANT THINGS TO KNOW ABOUT THIS DOCUMENT

- This document provides a **Policy** in the form of an assessment survey that defines the cybersecurity practices and processes third-party service and equipment vendors are expected to follow. After it is created, this Policy is expected to be authorized by your County and used for many years, even as your staff, vendors, and County continue to change.
- Once it is completed and authorized, this document will serve as **Your Policy** that you must adopt and adapt to the needs of **Your County**. SOS provides this template as a starting place, but you are expected to review and make changes, as appropriate for

your County. You, the **County Election Authority Leadership are ultimately responsible for the security of your election.**

  - Many of the actions and considerations defined in this Policy will apply to most Election Authorities. Depending on the needs of your organization, and depending on the vendors you engage, your Policy may have additional vendor security requirements and guidelines, or it may not have as many.
  - Some of the standards in this Policy template may not apply to you because of variations in facilities, organizational structure, and other factors, but you, the Election Authority must establish and adopt all of the vendor standards that are relevant to your organization.

- This Policy template must be reviewed and updated before use.
  - The template consists of areas that must be completed with details specific to your organization. These areas are pre-filled with suggestions or examples marked with underlined and *italicized* text.
  - You are encouraged to add your own specific policy instructions in the form of assessment survey items if you need to clarify or prescribe vendor practices or actions for purposes that are unique to your environment.
  - When you are ready to send the survey to your vendors to start the assessment process, you should review the assessment survey items and make sure they are appropriate for the services that a vendor provides for you. Some assessment survey items may not apply to the type of service and can be marked “Not Applicable” before the survey is sent.

INSTRUCTIONS FOR MAKING THIS DOCUMENT YOUR POLICY

1. Read through the entire policy template without making any changes, so you understand its full scope.
2. Read through the policy template again, this time marking each assessment survey item as belonging to one of the following categories:

- **Yes**

  Applies to you and no revisions are needed
- **Yes +**

  Applies to you, but needs to be refined with simple known revisions that make it more relevant
- **Maybe**

  Applies to you, but needs additional information that is not yet known or needs decisions that can only be made by someone else or a group of people
- **No**

  Does not apply to you because the standard references a process or resource that is not needed by your organization

3. Start working on adapting the policy to your specific criteria by making the needed revisions to the "Yes +" category.
4. Delete the assessment survey items that fall into the "No" category.
5. Gather the information needed for the "Maybe" category and obtain the needed decisions.
   - Delete an assessment survey item if a decision deems it no longer applicable to you and puts it in the "No" category.
   - Add decisions to your policy that fall into the "Yes" category.
6. Replace the underlined, italicized suggestions with your own details.

After you tailor the document to your election organization, it will become your **Vendor Risk Management Policy** and a part of your Election WISP. Follow the storage and document management processes for this document and for the rest of the Election WISP as defined in your Election Information Security Policy.

EVALUATION OF VENDOR SURVEY RESPONSES

You must review the responses vendors provide, and make sure that the descriptions are complete and include sufficient detail to determine whether vendor cybersecurity practices and physical security practices meet your County's Election Information Security Policy requirements. Perform analysis of the vendor responses by reviewing the descriptions they provide and comparing them to your Election Information Security Policy.

- You should look for a vendor's responses to contain details that meet or are similar to your Policy Statements and Policy Standards.
- If responses do not include specifics that address your Policy Standards, you should ask the vendors if they are able to make changes to meet your requirements.
- If a vendor's capabilities do not meet the requirements defined by your Election Information Security Policy, and if the vendor is unable or unwilling to make the required changes, you may need to consider alternatives. Or, if alternatives are not an option, you may have to accept the risks that the condition creates. These decisions should be documented.
- If items are not clear or do not adequately respond to the assessment survey item, you should ask vendors to revise their responses.

ASSISTANCE FROM TEXAS SOS ELECTION SECURITY TRAINERS

If you have questions or need help customizing this Vendor Risk Management Policy to your election organization and processes, contact the Texas Secretary of State Office at electionsecurity@sos.texas.gov to request assistance from an election security trainer.

DOCUMENT MANAGEMENT

The Vendor Risk Management Policy must be reviewed at least once per year or more frequently if state or federal legislation mandates new election security requirements. It should also be reviewed as new cyberthreats emerge, or when new vendors or organizational changes require plan updates between yearly reviews.

Maintain a record of all policy reviews in the Policy Review Log to validate that the Vendor Risk Management Policy is updated once per year and to track significant revisions. Record all review dates. If major revisions are made during the review, please describe the changes. If changes are not made during a review, note that no changes were made.

POLICY REVIEW LOG

POLICY ADOPTED DATE <Date>				
Drafted By	<Name, Title>	Signature	<Signature>	<Date>
Approved By	<Name, Title>	Signature	<Signature>	<Date>

<table>
<tr><td colspan="7">REVIEW AND REVISION LOG</td></tr>
<tr><td colspan="2">REVIEW SCHEDULE:</td><td colspan="5">General Election Years: December after elections
Legislative Session Years: July after SOS Law Conference</td></tr>
<tr><td colspan="7"></td></tr>
<tr><td>Review Date</td><td>If Revised, Revision Date</td><td>Revision Description (Or Specify “No Revisions” If None Made)</td><td>Drafted By: Name, Title</td><td>Signature, Date</td><td>Approved By: Name, Title</td><td>Signature Date</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

[Election Authority Name]

VENDOR RISK MANAGEMENT POLICY

CONTENTS

CONFIDENTIAL INFORMATION WARNING

This document contains information about the security of *[Election Authority Name]* that is classified as Confidential. Confidential information is any data that if disclosed could substantially harm the organization and its constituents, impede the conduct of effective government, law and order or violate citizen privacy. This data is exempt from disclosure under the provisions of the Texas Public Information Act and other applicable federal and state laws and regulations. It should only be shared with authorized individuals and should be strictly protected with access controls and security measures.

The following types of confidential information may be contained in this Policy:

System names and purposes

Security device configuration information

Procedural information that could be used to compromise agency systems

NON-DISCLOSURE STATEMENT

The information in this document is *[Election Authority Name]* Confidential, and cannot be reproduced, redistributed in any way, shape or form without prior written consent from *[Election Authority Name].*

INTRODUCTION

[Election Authority Name] uses information technology to manage and deliver services to our citizens and voters. The critical role that technology plays in election operations drives the need to protect the confidentiality, privacy, integrity, and availability of information and communications systems from cyberattack or other disruptive events. By evaluating the key cybersecurity practices implemented by third-party vendors, *[Election Authority Name] i*s able to ensure that security is at the foundation of all operations.

The **Vendor Risk Management Policy** is presented in the form of an assessment survey to provide a way to evaluate vendor cybersecurity practices and technologies. This helps to ensure that risks associated with outsourcing services and utilizing technology provided by third-party suppliers are understood and reduced where possible.

Each vendor must include a statement specifying that the vendor agrees to provide information in response to the Election Authority's ongoing cybersecurity reviews through the survey process.

SCOPE

This Policy is used to assess vendors that provide election services that may include, but are not limited to:

- Election management systems
- Ballot creation, printing, and programming services
- Ballot marking devices (BMDs) and direct-recording electronic (DRE) equipment used to capture votes
- Tabulation software systems
- Ballot scanner equipment
- Voter registration software systems
- Inventory management systems

- ePollbook technologies and management platforms
- Document scanning and management systems
- Website hosting platforms and providers
- Email hosting providers
- Election night reporting systems
- Other technology vendors and managed service providers

The Policy encompasses technology and ongoing services arrangements, including remote maintenance and access requirements, to help understand the full scope of third-party supplier risks and the need for risk assessments.

GOVERNANCE

The *[Election Administrator]* must ensure that vendors complete the assessment survey portion of the Vendor Risk Management Policy. Vendors are required to remediate any issues identified during the assessment process before working with *[Election Authority Name]*. If circumstances make it necessary to consider an exception, the *[Election Administrator]* is responsible for reviewing the risk and making a determination as to whether or not the vendor is allowed to implement an alternate practice or can be exempt from the requirement if the risk is determined to be accepted by the *[Election Administrator]*.

The Vendor Risk Management Policy enables *[Election Authority Name]* to meet requirements outlined in the Election Information Security Policy, specifically Policy 4: Supply Chain Risk Management.

POLICY 4: SUPPLY CHAIN RISK MANAGEMENT

Third-party vendors must comply with the Vendor Risk Management Policy included in the Election WISP.

POLICY STANDARDS

- The Vendor Risk Management Policy must be reviewed and updated, if needed, at least yearly as part of the Policy 1 Election WISP annual review requirement.

- Vendor risk assessment should be conducted annually by communicating with vendors to see if any significant changes to their networks, technologies, or business processes have recently occurred and by staying informed of cyberthreats that could affect vendors via the Information Sharing and Analysis Center (ISAC) subscription.
- All contracts, supply agreements, and service-level agreements will specify that the vendor agrees to comply with the Vendor Risk Management Policy.
- A staff escort is required for third-party vendors visiting facilities, and vendors who regularly work in our facilities are required to have identification badges that are not capable of opening doors or accessing secure areas.
- Vendor risk assessment will be evaluated annually as part of the Election WISP review described in the Policy.

The section that begins on the next page should be provided to vendors. Request that the vendor complete the survey with as much detail as possible.

Vendor Risk Management Policy and Assessment Survey

VENDOR INSTRUCTIONS

It is requested that [*the Vendor]* provide descriptions and examples, where applicable, that illustrate how your organization performs cybersecurity functions and otherwise enables capabilities that follow the *[Election Authority Name]* Vendor Risk Management Policy. Because your organization interacts with critical aspects of the supply chain and business process enablement for *[Election Authority Name],* your capabilities factor into the County's risks that may potentially include disclosure of voter registration information, invalidation of voter registration information, disruptions to the voting process, invalidation of the results of an election, or contribute to speculation about the validity, fairness, or accuracy of the election process.

Please complete the profile fields in the following assessment survey, and provide specific information related to how your organization supports *[Election Authority Name].*

This assessment survey is derived from the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The survey items provided are based upon an organizational risk scoring that evaluates the functionality that the services or products under consideration will provide. Scoring is conducted based upon factors that include the business criticality of the services and products; the types of data that will be stored, processed, transmitted or accessed via the service or products; and other risk factors such as legal and reputational risks to the organization.

Further information about the NIST Cybersecurity Framework can be found by visiting: https://www.nist.gov/cyberframework. This assessment survey is intended to provide information that will permit the Election Authority to evaluate the controls and environment that relate to the service or product under consideration. It is not *[Election Authority Name's]* recommendation or requirement that the company completing the assessment survey base its controls or security functions on the NIST Cybersecurity Framework.

COMPANY INFORMATION		
	Company Name	
	Name of Parent Company	
	Primary Business Address	
	Address of Production Data Center	
	Address of Backup Data Center	
	Other Addresses of Facilities Used in Providing Services or Products	
RESPONDER INFORMATION		
	Company Single Point of Contact Name	
	Title	
	Email	
	Phone	
ASSESSMENT SURVEY ITEMS		
IDENTIFY		
1	Describe how your organization actively tracks and manages authorized hardware devices and systems to ensure that unauthorized devices and systems are identified and prevented from gaining access.	
2	Describe how your organization actively tracks and manages authorized software to ensure that unauthorized software and applications are identified and prevented from installation or execution.	

3	Describe how your organization tracks and manages authorized data flows, application programming interfaces (APIs), and the extraction of data to ensure unauthorized access and removal of data does not occur.	
4	Describe how information resources are classified and categorized to ensure appropriate controls for protection and timely recovery, as well as for retention and planned destruction.	
5	Describe how your organization ensures that personnel have the required expertise and skills to perform their job duties and how they are trained on an ongoing basis to maintain required skills.	
6	Describe your organization's processes for identifying vulnerabilities within the information technology environment and network infrastructure and how remediation is performed to minimize exposure to threats and attackers.	
7	Describe how your organization tests the overall strength of defenses and simulates the actions of attackers, including penetration tests that are conducted periodically.	

8	Describe how your organization assesses, addresses, and accepts cybersecurity risks.	
9	Describe your organization's processes for managing the development, testing, and quality assurance of applications, software, and client configurations to ensure vulnerabilities within your products are identified and remediated.	
10	Describe the methodology and sources your organization uses to monitor the threat landscape and obtain cybersecurity threat intelligence and indicate if your organization participates as a member of the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC).	
11	Describe the assurance process your organization uses to evaluate cybersecurity risks and the capabilities within your organization's supply chain and supplier environment to mitigate them.	
12	Describe the extent to which your organization's suppliers, third-party providers, and customers are included in incident response planning and testing processes, or exercises conducted on a routine and periodic basis.	
PROTECT		

13	Describe how application accounts are requested, created, and maintained to ensure the appropriate data and system access permission levels for job duties are enforced. Also include information on how accounts are monitored for inappropriate activities, suspended when inactive, and removed when personnel change roles or employment is terminated.	
14	Describe how your organization facilitates remote access to its own IT systems, and whether multi-factor authentication is required for access at any level.	
15	Describe how your organization facilitates remote access to support client systems or devices, and whether multi-factor authentication is used to protect access.	
16	Describe how your organization tracks and approves authorization and permissions for access to its own IT systems and information. Include all levels of categorization/classification to ensure that personnel, systems, and applications only have access as approved and are limited to the least access that is needed to fulfill the job functions.	
17	Describe how your organization limits access to network ports, protocols, and services on network	

	devices, and how it utilizes segmentation to minimize vulnerabilities between systems/networks.	
18	Describe any access that is provided using a shared account ID accessible to more than one individual user.	
19	Describe how personally identifiable information (PII) and/or information that is deemed confidential or regulated is encrypted when at rest.	
20	Describe how personally identifiable information (PII) or information that is deemed confidential or regulated is encrypted when transmitted.	
21	Describe how data loss and leaks of information are prevented or detected.	
22	Describe how data and devices are protected, including how tamper-evident protections are used to ensure the integrity of software and hardware during shipment and transport to customer locations when supplied by the organization.	
23	Describe the process used for implementation and ongoing maintenance to prevent, detect, and correct security weaknesses in developed and acquired systems.	
24	Describe how information is backed up, stored and retained, and tested	

	periodically for restoration and recovery.	
25	Describe the physical security characteristics and access control measures of data center environments and facilities associated with data processing for the organization.	
26	Describe the organization’s availability, uptime, and failover processes and standard measures of performance.	
27	Describe the vetting process your organization uses during the personnel selection and onboarding process, as well as any periodic ongoing checks of personnel backgrounds.	
28	Describe how your organization conducts security awareness training for the organization as well as specific training for roles associated with privileged users.	
29	Describe your organization’s policy on collection, retention, and review of audit/event log records.	
30	Describe the processes used to define, implement, and maintain standard configurations and hardened configuration settings for your organization’s technology systems.	

31	Describe the protections your organization deploys to reduce the attack surface exposed to end users through email, internet websites, and social media.	
32	Describe the protections your organization uses to secure and prevent unauthorized access to Wi-Fi networks.	
DETECT		
33	Describe the process your organization uses to monitor events and analyze cybersecurity threats, attacks and suspicious activity.	
34	Describe how your organization prevents the installation, spread, and execution of malicious code and utilizes layers of defense to maximize automation to enable rapid updating of protections against quickly evolving malicious code.	
RESPOND		
35	Describe how your organization implements incident response plans as well as how it manages incidents as they are detected and responded to. Include how your organization uses lessons learned and proactive reviewing and testing to continually improve processes and protection capabilities.	
RECOVER		

36	Describe your organization’s implementation of the continuity of operations plan and how this plan is managed once activated.	

From: Christina Adkins
To: "Laura Stowe"
Subject: RE: SB 545 & SB 1070 implementation
Date: Tuesday, September 19, 2023 8:16:33 AM

Laura, my apologies.

We've been buried in audit activities and this email slipped through the cracks. SB 545 codified the process that was already in place with the Department of State Health Services regarding deceased individuals so this process continues to be in place and has been working well. With regard to SB 1070, we are looking at various sources of data, including working directly with other states, to meet the requirements of this provision. We don't want to be dependent on any one organization for list maintenance activities.

Let me know if you need more details on either of these bills.

Thanks,

Christina

From: Laura Stowe <Laura.Stowe@senate.texas.gov>
Sent: Tuesday, September 19, 2023 8:02 AM
To: Christina Adkins <CAdkins@sos.texas.gov>
Subject: RE: SB 545 & SB 1070 implementation

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 send this email as an attachment to Informationsecurity@sos.texas.gov.

Good Morning,

Hope your week is going well! Implementation may still be in progress so happy to let constituent know SOS is currently working out a plan on this. I did see some articles that suggested SOS was developing their own system to check voter rolls.

Best,

Laura Dally Stowe
Legislative Director
Office of Honorable Bob Hall
Senate District 2
Texas State Capitol, 4E.2
P.O. Box 12068
Austin, Texas 78711
Tel: 512-463-0102

From: Laura Stowe
Sent: Monday, September 11, 2023 10:21 AM
To: cadkins@sos.texas.gov
Subject: SB 545 & SB 1070 implementation

Good Morning,

Hope you had a great weekend!

I was hoping to get an update on the implementation status of SB 545 by Kolkhorst and SB 1070 by Hughes regarding voter rolls. We've had constituents reach out concerned with how voter rolls with be cleared/cleaned since moving away from ERIC.

Thanks so much!

Laura Dally Stowe
Legislative Director
Office of Honorable Bob Hall
Senate District 2
Texas State Capitol, 4E.2
P.O. Box 12068
Austin, Texas 78711
Tel: 512-463-0102

From: Keith Ingram
To: Grandjean, Amanda; Kristi Hart
Subject: Re: Subcommittee and Working Group Updates
Date: Thursday, June 22, 2023 3:27:20 PM
Attachments: image001.png

Kristi Hart is our technical point of contact.

Get Outlook for iOS

From: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
Sent: Thursday, June 22, 2023 09:31
To: Grandjean, Amanda <agrandjean@OhioSOS.Gov>
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 send this email as an attachment to Informationsecurity@sos.texas.gov.

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

image

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 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 them here. 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