Tuesday, July 21, 2026 at 12:02:40 PM Eastern Daylight Time

Subject: [Document Released to Requester] Unified Government of WYCO/KCK public records request #26-3254
Date: Tuesday, July 21, 2026 at 9:40:10 AM Eastern Daylight Time
From: Unified Government of WYCOKCK Public Records
To: AO Records
Category: PRODUCTION

EXTERNAL SENDER

-- Attach a non-image file and/or reply ABOVE THIS LINE with a message, and it will be sent to staff on this request. --

Unified Government of WYCO/KCK Public Records

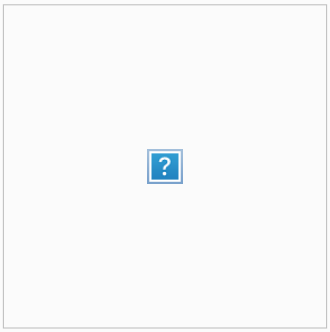
Documents have been released to you for record request #26-3254:

- [TLPCLEAR] CISA and Partners Release Fact Sheet on Securing Automatic Tank Gauge Systems.pdf
- [TLPCLEAR] CISA and Partners Release Fact Sheet on Securing Automatic Tank Gauge Systems_1.pdf
- [TLPCLEAR] CISA Launches CI Fortify Strengthening Resilience Across America's Critical Infrastructure.pdf
- [TLPCLEAR] CISA Launches CI Fortify Strengthening Resilience Across America's Critical Infrastructure_1.pdf
- GETSWPS Preparation - World Cup.pdf

View Request 26-3254

https://wycokck.nextrequest.com/requests/26-3254

AMERICAN OVERSIGHT



Questions about your request? Reply to this email or sign in to contact staff at Unified Government of WYCO/KCK.

Technical support: See our help page

AMERICAN OVERSIGHT

From: cyberliaisonsltt@cisa.dhs.gov
To: Mora, Elizabeth
Subject: [TLP:CLEAR] CISA and Partners Release Fact Sheet on Securing Automatic Tank Gauge Systems
Date: Wednesday, June 3, 2026 9:16:38 AM
Attachments: 1780494835653-0dknbvs-inline_image_1780494836060_0.png
1780494837679-k9zk9z0-inline_image_1780494838466_1.png

Greetings SLTT partners,

Today, CISA and federal partners released the fact sheet CISA and Partners Urge Hardening Automatic Tank Gauge Systems in response to malicious cyber activity targeting U.S. automatic tank gauge (ATG) systems, which are widely used across critical infrastructure sectors.

The recent malicious cyber activity observed by the authoring organizations—which the U.S. government has not yet attributed to a nation-state or threat actor group—involves cyber threat actors compromising internet-exposed ATG systems and subsequently modifying them through command execution.

This fact sheet provides insight into probable tactics, techniques, and procedures (TTPs) leveraged by these cyber actors, highlights risk factors associated with such compromises, and provides mitigation guidance and resources to reduce the likelihood of continued malicious activity targeting U.S.-based ATG systems.

Recommended Actions:

- Remove ATG systems from public internet exposure

AMERICAN OVERSIGHT

- Enforce strong, unique passwords and multifactor authentication
- Apply vendor patches and update software
- Monitor for unauthorized access and suspicious activity

For more information, review the full fact sheet. Report suspicious activity to CISA's Operations Center (report@cisa.gov or 888-282-0870) and the FBI's IC3 (www.ic3.gov).

Please share your thoughts with us through this anonymous survey. We appreciate your feedback.

Sincerely,



CyberLiaison SLTT
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Division | Joint Cyber Defense Collaboration (JCDC)
SLTT Partnerships | CyberLiaisonSLTT@cisa.dhs.gov

https://www.cisa.gov/tlp

TLP:CLEAR - please note that this message is marked TLP:CLEAR. We encourage you to share it within your organization and with your partners.

AMERICAN OVERSIGHT

From: cyberliaisonsltt@cisa.dhs.gov
To: Abbott, Michael G.
Subject: [TLP:CLEAR] CISA and Partners Release Fact Sheet on Securing Automatic Tank Gauge Systems
Date: Wednesday, June 3, 2026 9:32:15 AM
Attachments: 1780494835653-0dknbvs-inline_image_1780494836060_0.png
1780494837679-k9zk9z0-inline_image_1780494838466_1.png

Greetings SLTT partners,

Today, CISA and federal partners released the fact sheet CISA and Partners Urge Hardening Automatic Tank Gauge Systems in response to malicious cyber activity targeting U.S. automatic tank gauge (ATG) systems, which are widely used across critical infrastructure sectors.

The recent malicious cyber activity observed by the authoring organizations—which the U.S. government has not yet attributed to a nation-state or threat actor group—involves cyber threat actors compromising internet-exposed ATG systems and subsequently modifying them through command execution.

This fact sheet provides insight into probable tactics, techniques, and procedures (TTPs) leveraged by these cyber actors, highlights risk factors associated with such compromises, and provides mitigation guidance and resources to reduce the likelihood of continued malicious activity targeting U.S.-based ATG systems.

Recommended Actions:

- Remove ATG systems from public internet exposure

AMERICAN OVERSIGHT

- Enforce strong, unique passwords and multifactor authentication
- Apply vendor patches and update software
- Monitor for unauthorized access and suspicious activity

For more information, review the full fact sheet. Report suspicious activity to CISA's Operations Center (report@cisa.gov or 888-282-0870) and the FBI's IC3 (www.ic3.gov).

Please share your thoughts with us through this anonymous survey. We appreciate your feedback.

Sincerely,



CyberLiaison SLTT
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Division | Joint Cyber Defense Collaboration (JCDC)
SLTT Partnerships | CyberLiaisonSLTT@cisa.dhs.gov

https://www.cisa.gov/tlp

TLP:CLEAR - please note that this message is marked TLP:CLEAR. We encourage you to share it within your organization and with your partners.

AMERICAN OVERSIGHT

From: cyberliaisonsltt@cisa.dhs.gov
To: Mora, Elizabeth
Subject: [TLP:CLEAR] CISA Launches CI Fortify: Strengthening Resilience Across America's Critical Infrastructure
Date: Tuesday, May 5, 2026 2:06:12 PM
Attachments: 1778006696568-zssh4l3-inline_image_1778006696068_0.png

---

Greetings SLTT Partners,

Today, CISA announced CI Fortify: Strengthening Resilience Across Critical Infrastructure, a nationwide initiative that provides guidance to bolster the resilience of critical infrastructure against escalating cyber threats.

America's critical infrastructure (CI) is frequently targeted by malicious nation-state cyber actors. These adversaries seek persistent access to vital systems and aim to disrupt essential services such as telecommunications, water, energy, and transportation. To address these threats, CI organizations must be able to operate through a crisis or conflict; continuing vital service delivery even as their systems are under attack.

CI Fortify is a solution for emergency planning designed to address significant threat actor capabilities. These adversaries aim for more than espionage. To win a wider geopolitical conflict:
● They have successfully pre-positioned across critical infrastructure to disrupt and destroy the operational technology (OT) running the United States.
● They could leverage access to telecommunications infrastructure to take out phone and internet services.

The CI Fortify objectives result in a stronger, more resilient infrastructure capable of defending against a broad spectrum of threats and maintaining critical operations during emergencies:
● Operators will benefit from more control over connectivity in their infrastructure, as well as an easier to defend architecture, even in the absence of a nation-state conflict.
● Proactive emergency planning prepares operators to handle communication outages efficiently, whether caused by cybersecurity incidents, weather events, or other crises.
● Isolation disconnects command and control networks for threat actors already in the network.

The CI Fortify webpage is the central resource for CI Fortify guidance and updates; follow along as new CI Fortify resources will be published throughout the year. Stay informed and take action to strengthen your organization's resilience.

CISA strongly encourages organizations to review this guidance, implement the recommended actions, and collaborate with CISA to strengthen CI defenses against opportunistic threat actors.

Thank you,

AMERICAN OVERSIGHT



Cyber Liaison SLTT
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Division | Joint Cyber Defense Collaboration (JCDC)
SLTT Partnerships | cyberliaisonsltt@cisa.dhs.gov

AMERICAN OVERSIGHT

From: cyberliaisonsltt@cisa.dhs.gov
To: Abbott, Michael G.
Subject: [TLP:CLEAR] CISA Launches CI Fortify: Strengthening Resilience Across America's Critical Infrastructure
Date: Tuesday, May 5, 2026 2:23:39 PM
Attachments: 1778006696568-zssh4l3-inline_image_1778006696068_0.png

---

Greetings SLTT Partners,

Today, CISA announced CI Fortify: Strengthening Resilience Across Critical Infrastructure, a nationwide initiative that provides guidance to bolster the resilience of critical infrastructure against escalating cyber threats.

America's critical infrastructure (CI) is frequently targeted by malicious nation-state cyber actors. These adversaries seek persistent access to vital systems and aim to disrupt essential services such as telecommunications, water, energy, and transportation. To address these threats, CI organizations must be able to operate through a crisis or conflict; continuing vital service delivery even as their systems are under attack.

CI Fortify is a solution for emergency planning designed to address significant threat actor capabilities. These adversaries aim for more than espionage. To win a wider geopolitical conflict:
● They have successfully pre-positioned across critical infrastructure to disrupt and destroy the operational technology (OT) running the United States.
● They could leverage access to telecommunications infrastructure to take out phone and internet services.

The CI Fortify objectives result in a stronger, more resilient infrastructure capable of defending against a broad spectrum of threats and maintaining critical operations during emergencies:
● Operators will benefit from more control over connectivity in their infrastructure, as well as an easier to defend architecture, even in the absence of a nation-state conflict.
● Proactive emergency planning prepares operators to handle communication outages efficiently, whether caused by cybersecurity incidents, weather events, or other crises.
● Isolation disconnects command and control networks for threat actors already in the network.

The CI Fortify webpage is the central resource for CI Fortify guidance and updates; follow along as new CI Fortify resources will be published throughout the year. Stay informed and take action to strengthen your organization's resilience.

CISA strongly encourages organizations to review this guidance, implement the recommended actions, and collaborate with CISA to strengthen CI defenses against opportunistic threat actors.

Thank you,

AMERICAN OVERSIGHT



Cyber Liaison SLTT
Cybersecurity and Infrastructure Security Agency (CISA)
Cybersecurity Division | Joint Cyber Defense Collaboration (JCDC)
SLTT Partnerships | cyberliaisonsltt@cisa.dhs.gov

AMERICAN OVERSIGHT

From: PTS Service Center
Subject: GETS/WPS Preparation - World Cup
Date: Wednesday, June 17, 2026 11:14:51 AM

You don't often get email from gets.wps.support@cisa.dhs.gov. Learn why this is important

GETS/WPS POC,

CISA reminds all GETS/WPS Points of Contact (POCs) to encourage their subscribers to test their **Wireless Priority Service (WPS)** and **Government Emergency Telecommunications Service (GETS)** calling capabilities before the **FIFA World Cup**.

High-density environments surrounding this event are expected to generate **significant spikes in commercial network congestion**. WPS and GETS help ensure priority communications access during periods of network congestion.

Action Requested

All GETS/WPS POCs should:

1. **Confirm all operational personnel have access to WPS and GETS.**
2. **Ensure personnel verify WPS functionality** by placing a test call (e.g., *272 + 10-digit number).
3. **Verify that deployed personnel possess an active GETS PIN**, particularly those with landline or fixed-infrastructure roles.
4. **Submit any new enrollments or updates immediately** to ensure readiness before the event begins. Log in here to get started: https://www.gwids.cisa.gov/

Support

For enrollment questions, changes to POCs, or technical support, contact the Priority Telecommunications Service Center at gets.wps.support@cisa.dhs.gov, 866-627-2255, or 703-676-2255. Further information is available at http://www.cisa.gov/about-pts.

Timely action now ensures your agency remains fully mission-capable during this event.

Regards,

The PTS Service Center Team

AMERICAN OVERSIGHT