



# Water Sector Cybersecurity Regulatory & Resource Update

June 2024

# West Yost Associates Background

## West Yost Purpose

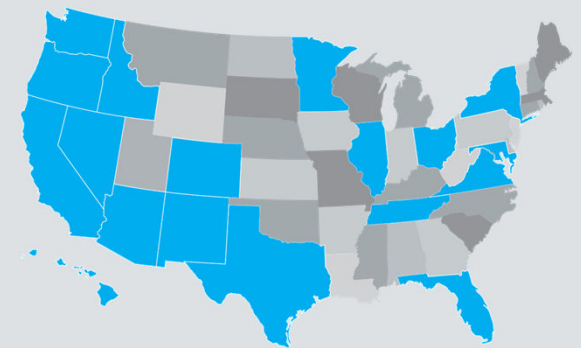
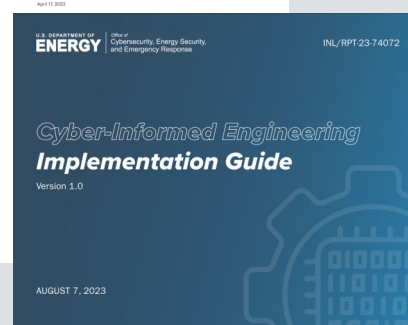
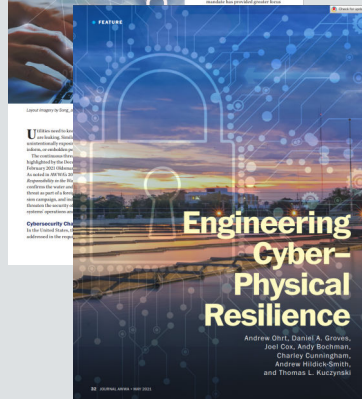
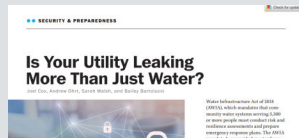
To advance water resources for future generations.

## West Yost Vision

To be the leader in water in the West.

## Water/Wastewater Focused

- 230 staff
- Operating across 19 states



# West Yost Support for USET & Members

- 2022 Cyber-Incident Response Planning – Virtual Training & Exercising
- 2022 TUS Presenter
- 2023 TUFF Presenter

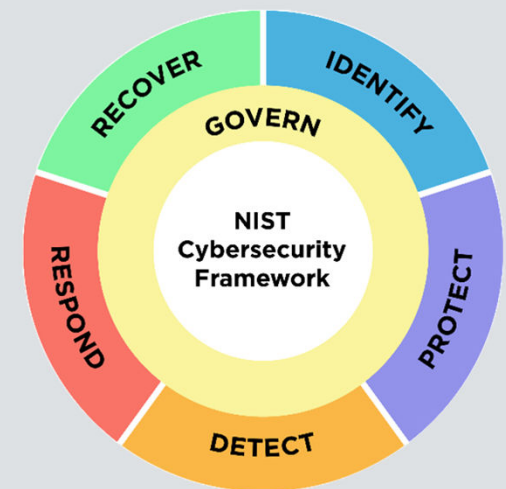


# Upcoming USET Virtual Cybersecurity Training!

Objective: Support USET Tribal Nation members to build capabilities to respond to a cyber-attack using cybersecurity and emergency preparedness best practices.

## Schedule:

- Thursday, August 8<sup>th</sup> – Introduction/Govern
- Thursday, August 22<sup>nd</sup> – Prepare/Prevent
- Thursday, August 29<sup>th</sup> – Detect
- Tuesday, September 10<sup>th</sup> – Respond
- Thursday, September 19<sup>th</sup> – Recover
- Thursday, September 26<sup>th</sup> – Virtual Tabletop Exercise!





# Our Challenge

USET | June 2024

# Oldsmar – February 2021



**Security**  
**Water treatment plant hacked, chemical mix changed for tap supplies**  
 Well, that's just a little scary


By John Leyden 24 Mar 2016 at 12:19

Hackers infiltrated a water utility's control system and changed the level of chemicals being used to treat tap water. We're frid

82 SHARE

**Riviera Beach, Florida Ransomware Attack: City Pays \$600,000**  
 A Riviera Beach, Florida, ransomware attack prompted the city to pay \$600,000 to hackers in a bid to decrypt infected systems.

by DH Kass • Jun 20, 2019



**BWL paid \$25,000 ransom after cyberattack**

Ken Palmer, Lansing State Journal

Published 9:32 p.m. ET Nov. 8, 2016 | Updated 4:26 p.m. ET Nov. 10, 2016

CONNECT TWEET LINKEDIN COMMENT EMAIL MOBILE

LANSING - The Lansing Board of Water and Sanitation (BWL) paid a \$25,000 ransom to unlock its water communications system after a cyberattack last week.

**BeaverCountian.com**

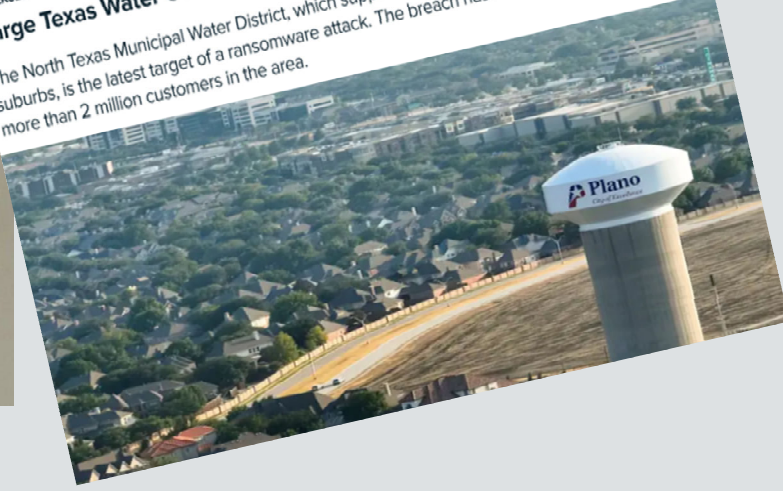
HOME LOG IN SUBSCRIPTION ABOUT CONTACT

**Iranian-Linked Cyber Army Had Partial Control Of Aliquippa Water System**

by John Paul | Nov 25, 2023

**CYBERSECURITY**  
**Large Texas Water Utility Hit With Ransomware Attack**

The North Texas Municipal Water District, which supplies water to sprawling Collin County suburbs, is the latest target of a ransomware attack. The breach has not disrupted service to the more than 2 million customers in the area.



 **United States Attorney's Office**  
 District of Kansas

**PRESS RELEASE**  
**Kansas Man Pleads Guilty to Tampering with Public Water System**

Thursday, October 21, 2021

TOPEKA, KAN. – A Kansas man pleaded guilty to tampering with a public water system in Ellsworth County. Wyatt Travnichek, 23, of Lorraine pleaded guilty to one count of tampering with a public water system and one count of reckless damage to a protected computer system during unauthorized access.



GEOPOLITICS

# Mandiant: Not breach of Texas

Researchers from the Good  
recent attacks on critical i

BY AJ VICENS AND CHRISTIAN VASQUEZ

# Inc.

NEWSLETTERS

SECURITY

## FBI Warns on Chinese Cyberattacks as Texas Towns Report Russian Hacks on Water Systems

State-backed attacks on U.S. infrastructure are increasing, and federal law enforcement calls out China's "Volt Typhoon" hacking campaign.

BY REUTERS  
APR 19, 2024



FBI Director Christopher Wray. Photo: Getty Images

g unit linked to

personas are linked to several

# Russia-linked targeted Inc



By Sean Lyngaas, CNN  
⌚ 2 minute read · Published

# claims to have

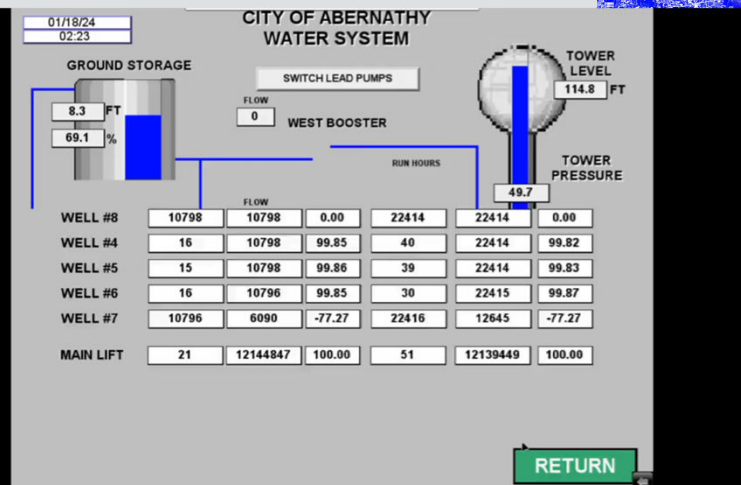


# Recent Incidents in the Water/Wastewater Sector

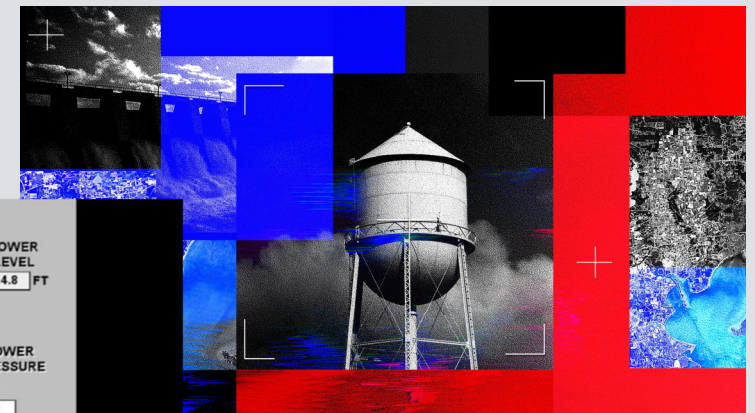
BY ANDY GREENBERG SECURITY APR 17, 2024 6:00 AM

## Hackers Linked to Russia's Military Claim Credit for Sabotaging US Water Utilities

Cyber Army of Russia Reborn, a group with ties to Kremlin's Sandworm unit, is crossing lines even that notorious cyberwarfare unit wouldn't dare to.



<https://www.wired.com/story/cyber-army-of-russia-reborn-sandworm-us-cyberattacks/>



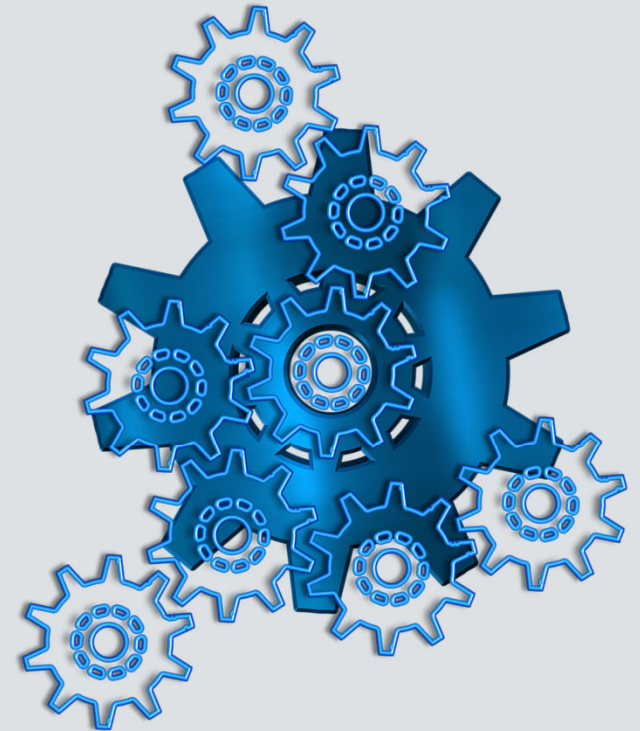


# Regulatory Update

USET | June 2024

# Select Policy Actions

- 💧 ***EPA Sanitary Survey Cyber Rule***
  - 💧 *EPA issued March 3, 2023*
  - 💧 *Legal challenge filed by MO, AR, IO, joined by AWWA, NRWA*
  - 💧 *Nationwide injunction July 12, 2023*
  - 💧 *Withdrawn by EPA on October 12, 2023*
- 💧 ***National Security Council Letter to Governors***
  - 💧 *Requested Governors provide a Water System Action Plan by June 28, 2024*
- 💧 ***AWIA §2013 round 2 pending***
  - 💧 *Enforcement action anticipated*



# Key Cyber Provisions in AWIA §2013 (SDWA §1433)

## Risk & Resilience Assessment

- **Must consider cyber threats to the system, which includes:**
  - *Electronic, computer, or other automated systems,*
  - *Monitoring practices of the system, and*
  - *Financial Infrastructure*

## Emergency Response Plan

- **Shall include:**
  - *Strategies and resources to improve the resilience of, physical & cybersecurity, the system*
  - *Actions, procedures, and equipment which can obviate or significantly lessen the impact of an incident*

# AWIA §2013 (SDWA §1433) Round 2

Community Water System (pop. served)*‡	Certify Risk & Resilience Assessment (RRA) by:	Certify ERP within 6 months of RRA, but not later than:
≥ 100,000	March 31, 2025	September 30, 2025
50,000 – 99,999	December 31, 2025	June 30, 2026
3,300 – 49,999	June 30, 2026	December 30, 2026

\* Wholesalers use population of all systems served

‡ Population as of March 31, 2024

# Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA)

## 💧 *Cyber Incident Reporting Rule*

- 💧 *Applies to CWS & POTW serving >3,300 persons*
- 💧 *Currently open for comments, due June 3, 2024*
- 💧 *Final rule by October 2025*

## 💧 *Cyber Incident Reporting Requirements*

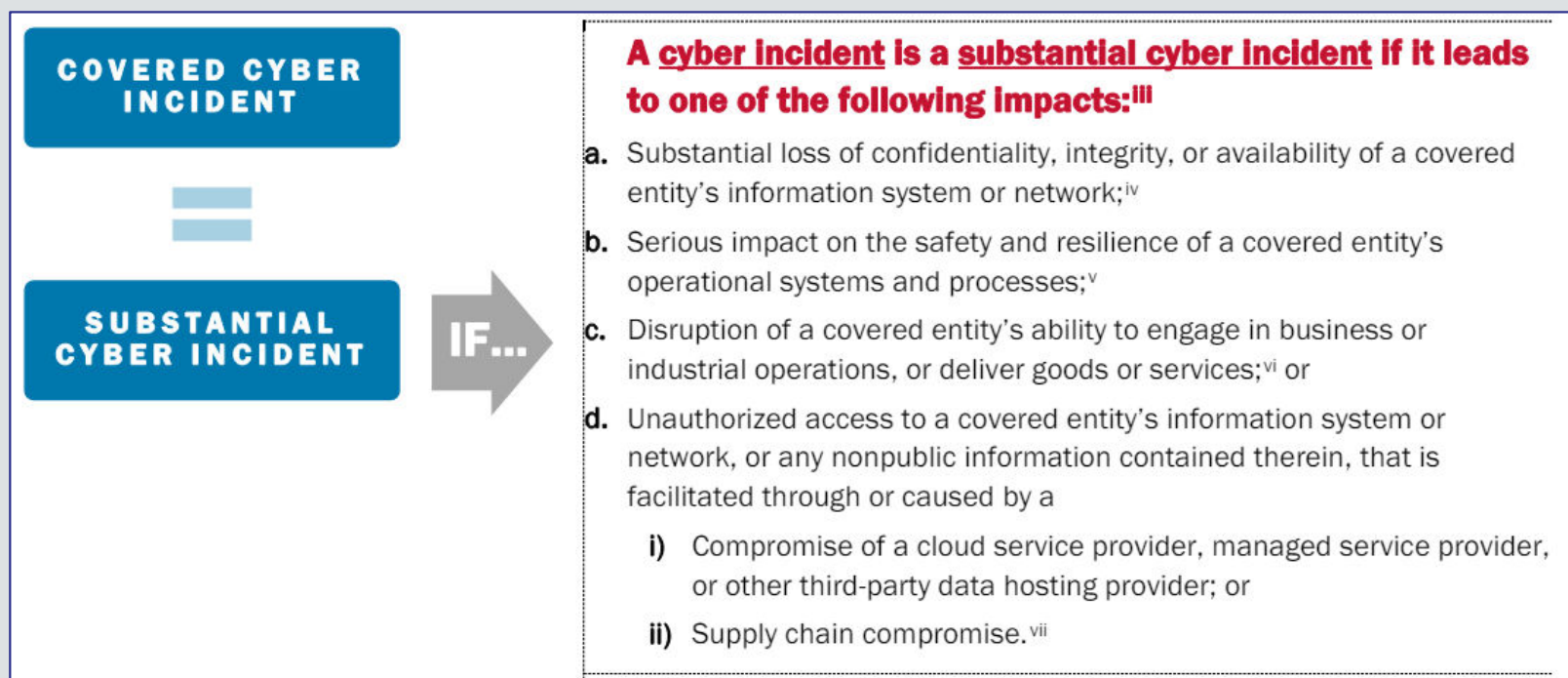
- 💧 *Covered entities must report to CISA any covered cyber incidents within 72 hours from the time the entity reasonably believes the incident occurred*

## 💧 *Ransomware Payment Reporting Requirements*

- 💧 *Covered entities must report to CISA within 24 hours of making any ransom payments made as a result of a ransomware attack*

# What is a Covered Cyber-Incident?

A covered cyber incident is a substantial cyber incident experienced by a covered entity





APRIL 30, 2024

# National Security Memorandum on Critical Infrastructure Security and Resilience

- Recognizes that the U.S. *“...faces an era of strategic competition with nation-state actors who target American critical infrastructure...”*
- Focus on minimum cross-sector requirements for security and resilience
- Expected outcomes:
  - Cross-sector Physical Security Goals
  - Additional funding for Water Sector cybersecurity improvements



# House of Representatives (H.R.) 7922

- *To establish a Water Risk and Resilience Organization (WRRO) to develop risk and resilience requirements for the water sector.*



# NERC Background



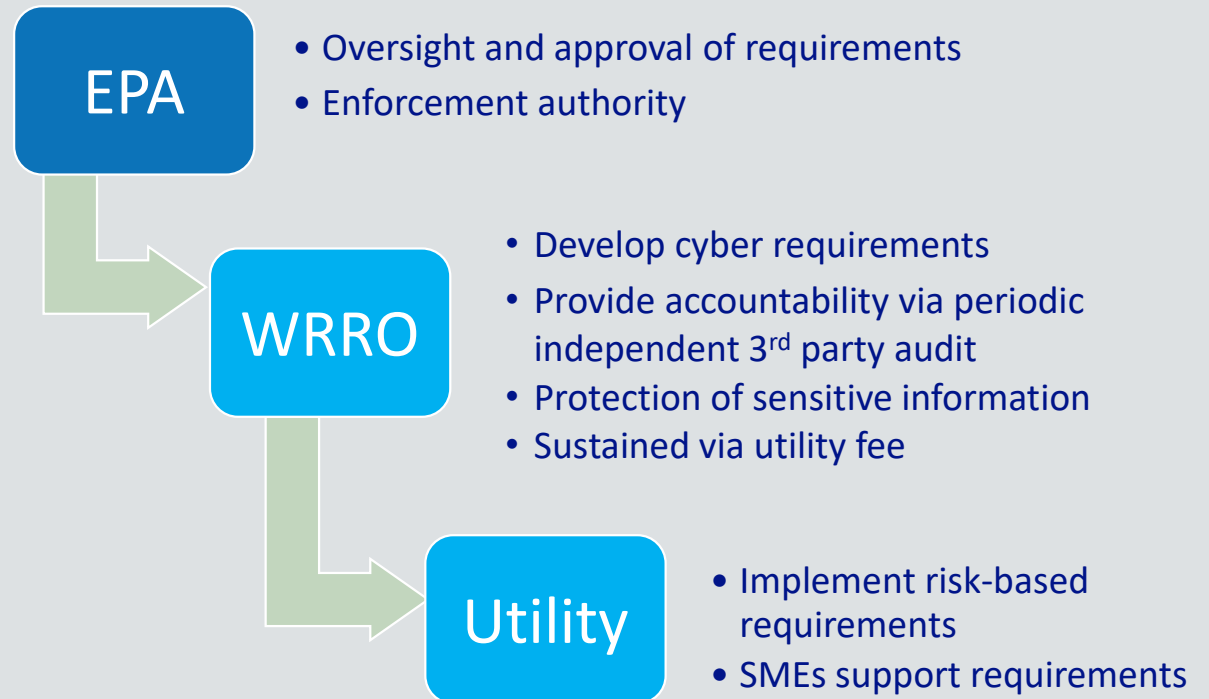
***Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the [bulk electric] grid.***



- 2005 – Energy Policy Act of 2005 – Authorized the creation of an audited, self-regulatory Electric Reliability Organization.
- 2006 – NERC Certified as the Electric Reliability Organization for the U.S.
- 2008 – The first version of NERC’s Critical Infrastructure Protection (CIP) Reliability Standards approved.

# H.R. 7922

*To establish a Water Risk and Resilience Organization (WRRO) to develop risk and resilience requirements for the water sector.*



# The WRRO Will:

1. Establish cybersecurity risk and resilience requirements for water systems to implement.
2. Establish a schedule for implementation of cybersecurity risk and resilience requirements.
3. Audit implementation of cybersecurity risk and resilience requirements.
4. Levee penalties on water systems who violate cybersecurity risk and resilience requirements

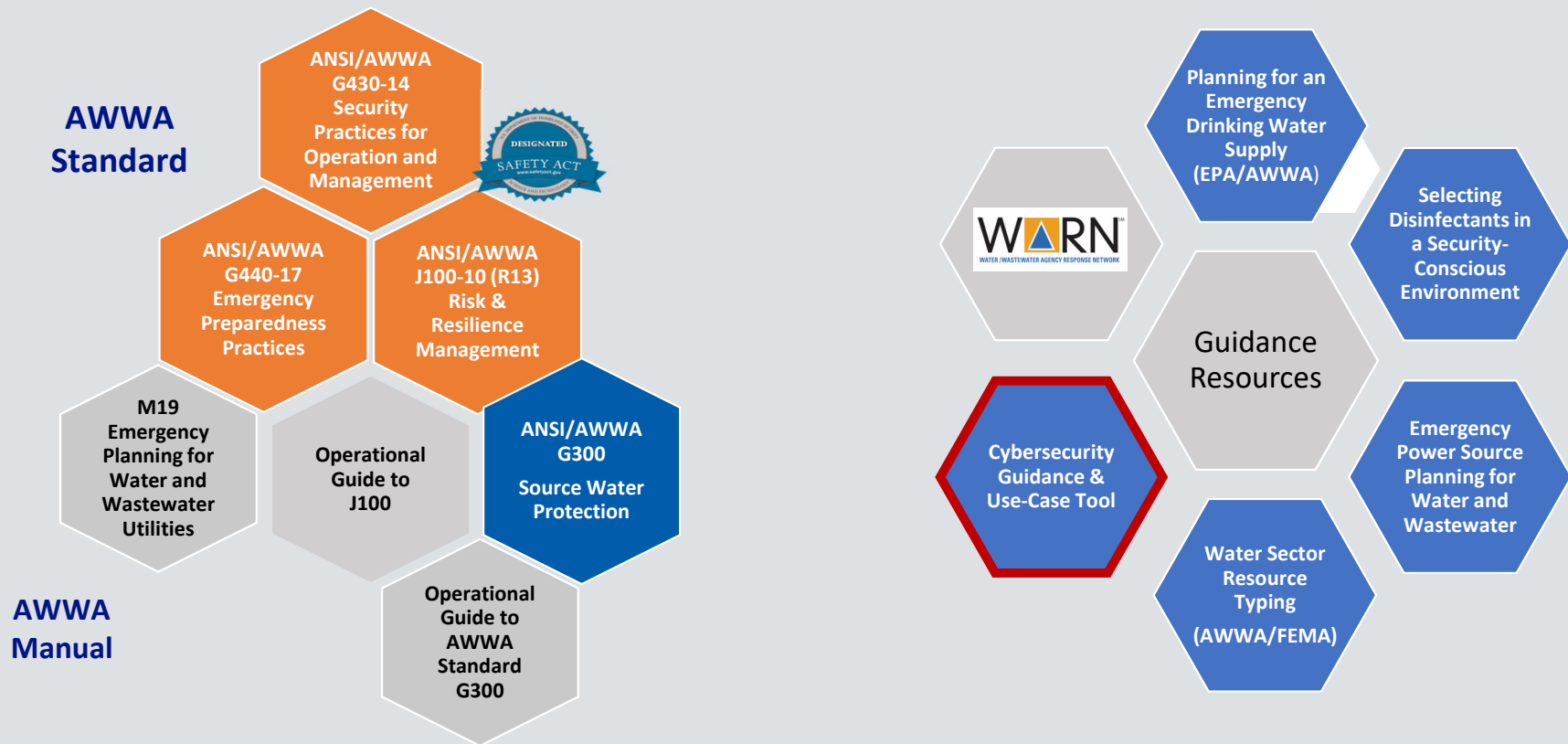


# Resource Update

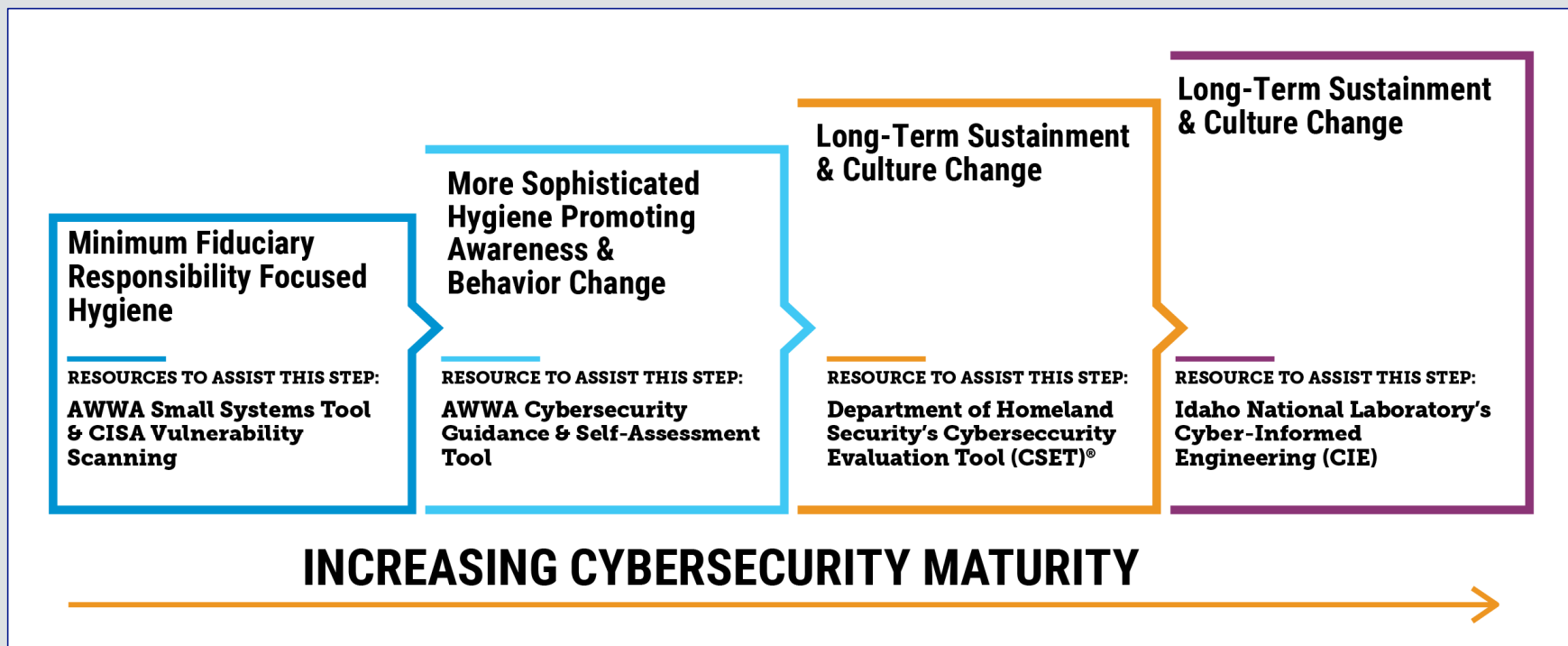
AWWA, EPA, CISA, & INL

USET | June 2024

# AWWA Risk & Resilience Resource Suite



# AWWA Cyber Maturity Model



# CISA Vulnerability Scanning

## Cyber Hygiene Services

### Reducing the Risk of a Successful Cyber Attack

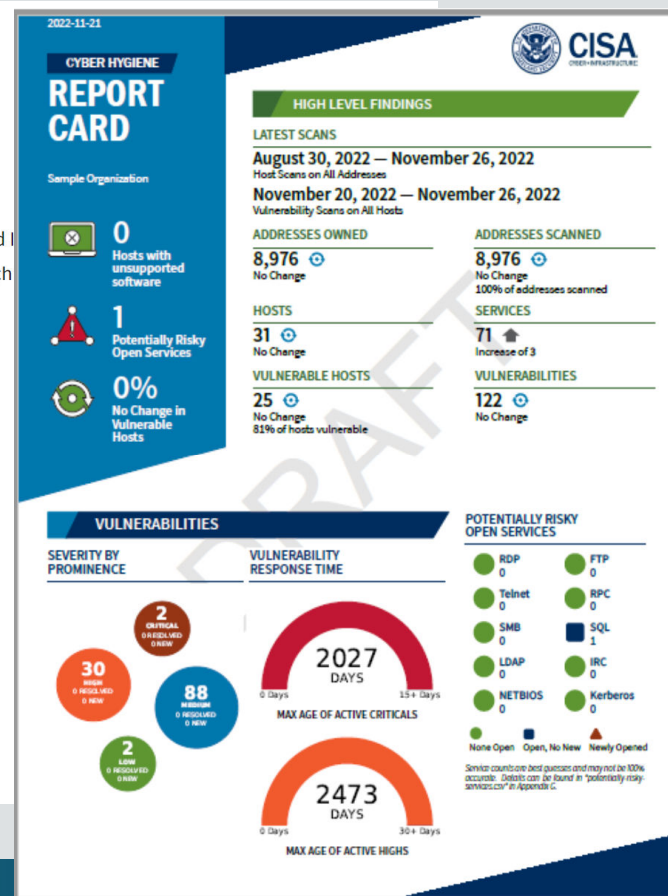
Adversaries use [known vulnerabilities and weaknesses](#) to compromise the security of organizations. The Cybersecurity and Hygiene scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach

EMAIL US TO ENROLL TODAY →

CISA's available Cyber Hygiene services are listed below:

- **Vulnerability Scanning:** Evaluates external network presence by executing continuous scans of public, static IPv4s for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Web Application Scanning:** Evaluates publicly accessible web applications to uncover vulnerabilities and misconfigurations that attackers might exploit. This comprehensive evaluation includes, but is not limited to, the vulnerabilities listed in the OWASP Top 10, which represent the most critical web application security risks. This service provides detailed reports on a monthly basis monthly, as well as on-demand reports to help ensure your web applications remain secure.

<https://www.cisa.gov/cyber-hygiene-services>





# EPA's Cybersecurity Resources

- Addressing Cybersecurity in your AWIA-compliant Emergency Response Plan
- Cybersecurity Guidance for Drinking Water and Wastewater
- Cybersecurity Risk Self-Assessment/Third-Party Resources
- Cybersecurity Vulnerability Assessment Resources
- Technical Assistance
- *Forthcoming guidance document.*

<https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector>



## U.S. EPA Water Sector Cybersecurity Evaluation Program

### How is the Cybersecurity Evaluation Program helping water and wastewater systems build cyber resilience?

The EPA will conduct a free cybersecurity assessment for Water/Wastewater Systems (W/WSs) to identify gaps or vulnerabilities in information technology (IT) and operational technology (OT) using the EPA Cybersecurity Checklist.

### What is the EPA Cybersecurity Checklist?

The Cybersecurity Checklist is a list of questions EPA derived from CISA's Cybersecurity Performance Goals to help W/WSs assess their cyber risk. The Cybersecurity Checklist is available in the EPA guidance document, EPA Cybersecurity Risk Assessment Guidance for Drinking Water and Wastewater Systems. W/WSs are encouraged to use the resources and technical assistance offered in EPA's guidance document to address identified gaps and reduce the risk of cyberattacks.

### How does the Cybersecurity Evaluation program work?

A W/WS must register to receive a cybersecurity assessment. Once registered, an EPA contractor will contact the W/WS to gather basic information, provide guidance on how to prepare and schedule an assessment. During the assessment, the EPA

contractor will ask the W/WS each of the questions in the Cybersecurity Checklist.

The contractor will generate a report that identifies cybersecurity gaps and/or vulnerabilities in the W/WS's IT/OT based on response to the Cybersecurity Checklist. In addition, a template for a Risk Mitigation Plan will be generated, which the W/WS can use to plan and document actions to address cybersecurity gaps.

### What does the W/WS need to prepare before the assessment?

The assessment will require input from management, operations, business, and IT and OT staff as appropriate. The W/WS will also need to compile any existing system documentation, diagrams, policies, and procedures to help answer the Checklist questions.

### How does EPA protect the results of the W/WS Cybersecurity Assessment?

EPA does not share the results of the assessment with any party beyond the W/WS. The file is delivered using a secure file transfer. The contractor shares the anonymized, aggregated results with EPA. EPA will protect information submitted to the agency in accordance with applicable authorities. The EPA contractor supporting this program is the Horsley Witten Group, Inc.

### To register your W/WS, please visit:

[www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program](https://www.epa.gov/waterresilience/forms/epas-water-sector-cybersecurity-evaluation-program)

### For more information, contact:

Horsley Witten Group  
508-833-6600 x501

Office of Water (4608T)  
EPA-810-F-24-003  
February 2024



# Cyber-Informed Engineering (CIE)

PRINCIPLE PHASE  
**1 A**

**PRINCIPLE 1: CONSEQUENCE-FOCUSED DESIGN**  
CONCEPT PHASE (continued)

**5 What business areas may be uniquely impacted by system failure or unexpected operation?**

- a Which parts of the business would be affected by each consequence?
- b Which resulting consequences could be categorized as "acceptable" and could be managed within organizational risk management processes?
- c Which consequences (physical or otherwise) are "unacceptable" and must be mitigated? Document these distinct consequences.

**6 What regional system failure**

- a What ent infrastruc
- b What cha from regi

**7 What crucial**

- a What viol

**8 Where might**

- a At each i

**9 Are there adv**

- a What circ
- b In advers conseque

**10 What staffing**

**What training**

- a Where mi support c
- b What are

**EXAMPLE:** Loss of control or disruption of a large power transformer within the bulk electric system (BES) could affect the transmission capacity of a regional electric power grid. Depending on the location, downstream effects could impact large population

First point in the Engineering Lifecycle that the example is considered  
Continuation of the example through the Engineering Lifecycle

PRINCIPLE	CIE CONTROL/MITIGATION
<b>Principle 6: Active Defense</b>	<p><b>6-1</b> Implement an OT network to support d Trust Architecture with</p> <p><b>6-2</b> Generate docum signs and how to doo connection/devices</p>
<b>Principle 7: Interdependency Evaluation</b>	<p><b>7-1</b> Implement confi relationships between communication durin</p> <p><b>7-2</b> Ensure multiple e on outside inputs.</p>
<b>Principle 8: Digital Asset Awareness</b>	<p><b>8-1</b> Adopt a commes solution that uses pe inventory.</p> <p><b>8-2</b> Regularly update found in the inventor</p>
<b>Principle 9: Cyber-Secure Supply Chain Controls</b>	<p><b>9-1</b> Include security r develop a Secure Sof implement tight vendor controls.</p>
<b>Principle 10: Planned Resilience</b>	<p><b>10-1</b> Install hardwired controls for all critical systems.</p> <p><b>10-2</b> Generate documentation and train staff to expect that any digital component can become compromised and lose functionality and know how to operate in manual.</p>

**PRINCIPLE 1**  
**Consequence-Focused Design**

**KEY QUESTION**  
**How do I understand what critical functions my system must ensure and the undesired consequences it must prevent?**

**Principle Description**  
Apply CIE strategies first and foremost to the most critical functions the system performs. Typically these are functions that, if manipulated or subverted, could result in unacceptable or catastrophic consequences for the organization, including undesired impacts to security, safety, quality, the environment, availability or effectiveness of products or services, system integrity, and public image. Use a structured and thorough process to identify areas where digital technology is used within these functions.

Consider where an unprotected action or failure of the function that leverages digital technology might lead to a high-consequence event. These could include unauthorized system actions, invalid data that would drive an automated action, or interdiction of a digitally governed control. Examine the controls that exist to minimize impacts of misuse or failure and whether those controls are implemented via digital technology, physical mechanisms, or a combination of both.

This list of high-impact consequences underpins the work engineers will perform throughout the system design lifecycle and the actions to be taken and their priority within each CIE principle. For each element identified in the work above, engineers will consider engineered controls (see Principle 2: Engineered Controls), that could either remove the possibility for the unprotected action or mitigate its consequences. These changes complement traditional cybersecurity protections to increase the overall resiliency of the system to undesired digital events that could result in catastrophic consequences.

**Consequence-Focused Design Considerations at Each Lifecycle**  
Because the Consequence-Focused Design principle provides key considerations, it should be the first principle considered at the beginning of the lifecycle phase. Consequence-Focused Design functions as a foundational principle that, once assessed, is used as the basis of considerations for other principles. At a high level, early considerations may focus on negative business consequences such as delivery failure, equipment damage, or impacts to safety, that may apply to the system generally. As the system matures, more specific considerations may be required, such as catastrophic consequences will require a stronger emphasis on consequence-focused design.

Specific elements considered in the Consequence-Focused Design principle will shift as the principle is applied across time and system maturity. It is important to note that the trajectory of industry and technology change may affect consequence assessment throughout a system's lifecycle. Consequence is a moving target that should be regularly reassessed as the considered system is not changing.<sup>4</sup>

<sup>4</sup> This idea aligns with ISA/IEC 62443 "Assess, Design & Implement, Operate & Maintain" 62443-3-2, which focuses on regular risk assessment for the System under Consideration. While the system may not have changed, the patches, updates, added users, third-party admin access to firewalls and switches, and organizational culture do often change, creating unconsidered consequences. The reassessment should also have externally vetted peer review to avoid internal company bias.

U.S. DEPARTMENT OF **ENERGY** Office of Cybersecurity, Energy Security, and Emergency Response

*Cyber-Informed Engineering*  
**Implementation Guide**

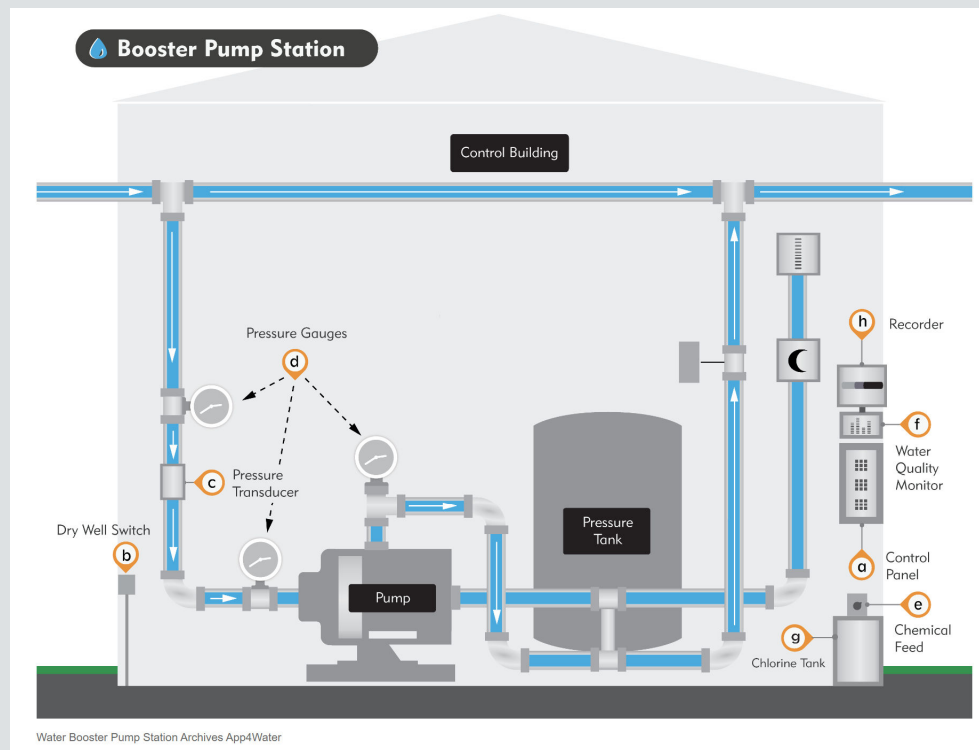
Version 1.0

**DRAFT**

AUGUST 7, 2023

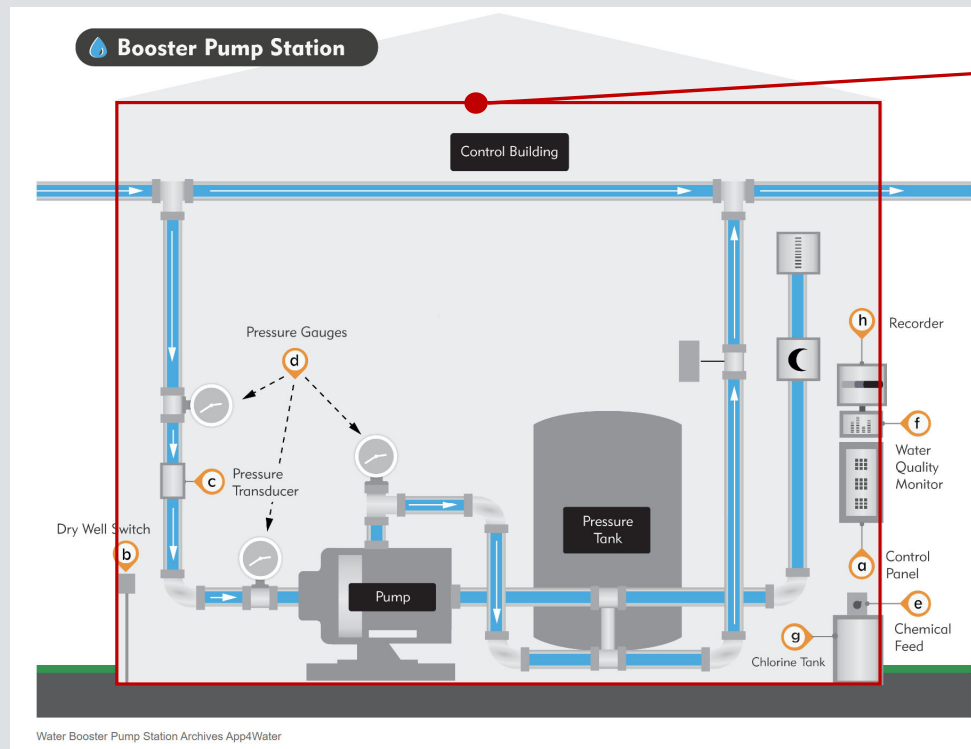
INL/RPT-23-74072

# Water Booster Pump Station



[https://bmxlovesk.xyz/product\\_details/13200675.html](https://bmxlovesk.xyz/product_details/13200675.html)

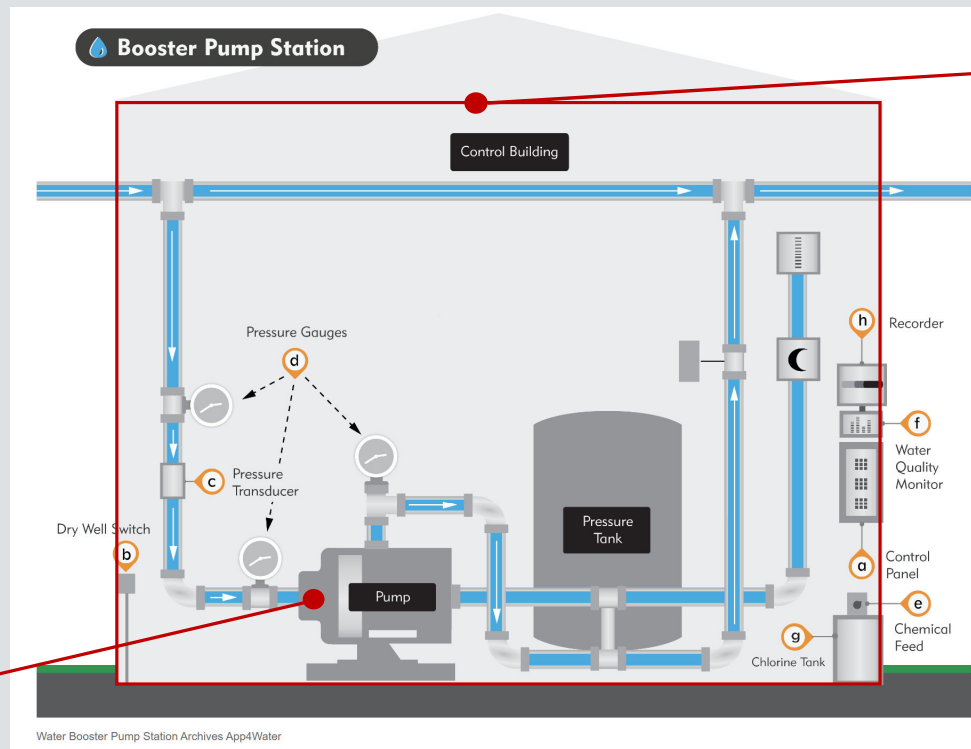
# Water Booster Pump Station



Cloud-based monitoring and control

[https://bmxlovesk.xyz/product\\_details/13200675.html](https://bmxlovesk.xyz/product_details/13200675.html)

# Water Booster Pump Station



Cloud-based monitoring and control

Mechanical Time Delay Relay

[https://bmxlovesk.xyz/product\\_details/13200675.html](https://bmxlovesk.xyz/product_details/13200675.html)

# Applying CIE to New Infrastructure

CIE Engineering  
Guidelines



30% Design  
Review



60% Design  
Review



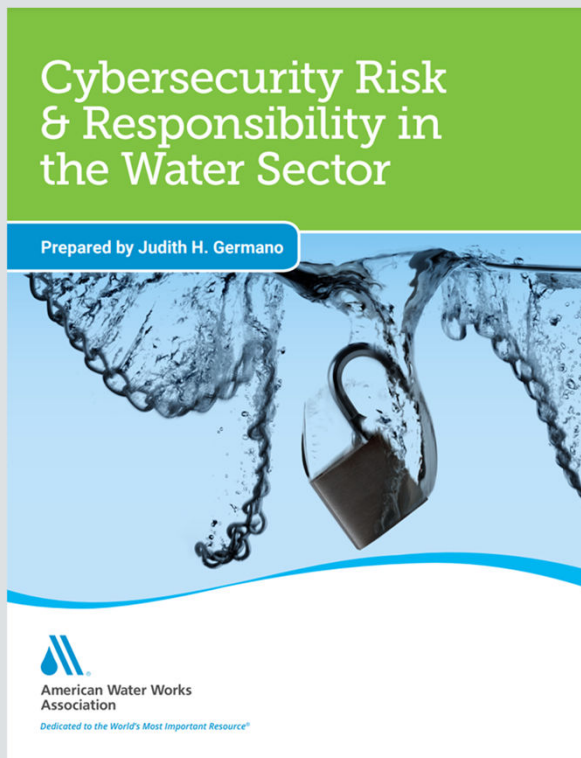
90% Design  
Review



## Key Concepts:

- Cyber-Enabled Failure Mode
- Commander's Intent

# Cybersecurity Risk & Responsibility



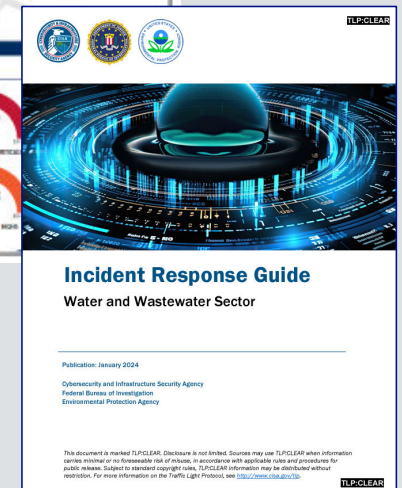
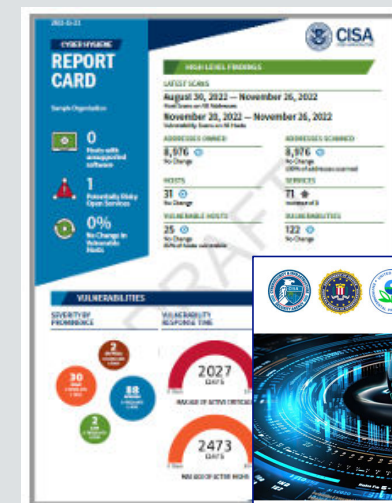
- Cyber Threats are Foreseeable
- Implement Best Practices
- Demonstrate Due Diligence
- Insurance & risk transfer
- **Fiduciary Responsibility**

# Conclusion



# No Action is No Good

- 💧 Educate staff on their role in protecting the mission from cyber threats
- 💧 Enroll in CISA's Vulnerability Scanning Service (Email CISA at [vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov))
- 💧 Implement multifactor-authentication
- 💧 Ensure all staff have unique usernames and strong passwords
- 💧 Get a .gov domain if tribal/local entity like a water systems (see [get.gov](https://www.get.gov))
- 💧 Develop an Incident Response Plan



# Upcoming USET Virtual Cybersecurity Training!

Objective: Support USET Tribal Nation members to build capabilities to respond to a cyber-attack using cybersecurity and emergency preparedness best practices.

## Schedule:

- Thursday, August 8<sup>th</sup> – Introduction/Govern
- Thursday, August 22<sup>nd</sup> – Prepare/Prevent
- Thursday, August 29<sup>th</sup> – Detect
- Tuesday, September 10<sup>th</sup> – Respond
- Thursday, September 19<sup>th</sup> – Recover
- Thursday, September 26<sup>th</sup> – Virtual Tabletop Exercise!



# Thank you!



## Andrew Ohrt, PE, CISSP

- Resilience Practice Area Lead
- (952) 303-9905
- [aohrt@westyost.com](mailto:aohrt@westyost.com)
- <https://www.linkedin.com/in/andrewohrt/>

The background features a dark, abstract digital landscape. It is composed of a complex network of thin, glowing lines in shades of green and blue. These lines form a wireframe-like terrain with rolling hills and valleys. Vertical lines of varying heights are scattered across the scene, resembling data points or signal towers. The overall aesthetic is futuristic and technological, with a gradient from dark green on the left to dark blue on the right.

# QUESTIONS

[WESTYOST.COM](http://WESTYOST.COM)