
INFORMATIONAL WEBINAR

Getting to Know WaterISAC

December 11, 2024



AGENDA

- WaterISAC Overview
- Policy Updates
- Cyber Threat Briefing
- Physical Threat Briefing
- Member Portal Information

DON'T FORGET!

We are recording and
the Q&A box is open
at all times!

WHO WE ARE

The [Water Information Sharing and Analysis Center](#) (WaterISAC) is the only all-hazards security information source for the water and wastewater sector. We now serve over 600 member companies and utilities with 3,900+ active water sector personnel. Our utility members provide water and wastewater services to Americans across the nation.

- Formed over 20 years ago by the sector's leading national associations at the urging of the White House, FBI, and EPA.
- Maintain two-way communication with DHS, FBI, EPA, fusion centers, and other federal, state, and local agencies in order to help protect and share information.
- Work to advance the security of the sector through critical and direct participation of industry meetings and working groups.



HOW IT WORKS



ALL THINGS WATERISAC - PRODUCTS

ALERTS



Stay in the know! We are in constant communication with CISA, DHS, EPA, FBI, and other government agencies to ensure members receive timely and actionable alerts.

ANALYSIS



Provide quarterly and annual reports analyzing cyber and physical incidents around the nation.

NEWSLETTERS



Twice-weekly newsletters, Security & Resilience Updates (SRU) curated by our analysts to provide focused content and best practices.

RESOURCES



Access to over 14,000 security resources for the water and wastewater sector.

ALL THINGS WATERISAC - EVENTS

- Monthly Events
 - Water Sector Cyber Resilience Briefing
- Quarterly Events
 - Water Sector Physical Threat Briefing
 - Water Sector Natural Disaster Threat Briefing
 - WaterISAC Informational Webinar
- H2OSecCon
- Other Events

POLICY UPDATES

- Election results
- Water Risk and Resilience Organization legislation
- Water Preparedness and Resilience legislation
- Proposed Cyber Incident Reporting rule

POLICY UPDATES

2024 Elections

- Trump wins Electoral College and popular vote
- Republicans take Senate with 53-47 advantage
- Republicans maintain narrow 220-215 House majority
- Democrats will have opportunities to block Trump agenda

POLICY UPDATES

Water Risk and Resilience Legislation

- Introduced in House of Representatives by Rep. Rick Crawford (R-Ark.) in April as H.R. 7922
- Would establish a WRRO comprised of water sector experts to develop tiered, risk-based cyber requirements for water and wastewater systems serving more than 3,300 people
- Could serve as “off the shelf” legislation if Congress decides to tackle water cybersecurity

POLICY UPDATES

Water Preparedness and Resilience legislation

- Introduced in the House and Senate in 2023 as H.R. 1367 and S. 660
- Would direct EPA to do more to promote WaterISAC to water and wastewater systems, and authorize funds to offset membership dues
- AMWA are positioning the bill to be part of any larger water cybersecurity package Congress may consider in the future

POLICY UPDATES

CIRCI – cyber incident reporting rule

- CISA proposed Cyber Incident Reporting for Critical Infrastructure Act (CIRCI) rule in April
- Covered critical infrastructure entities would have to report significant cyber incidents to CISA within 72 hours, or cyber ransom payments within 24 hours, but Congress barred enforcement against public entities
- AMWA comments requested clarity, and encouraged voluntary incident reporting through mechanisms like WaterISAC
- Regulation could be paused by anticipated Trump “regulatory freeze”

Cyber Threats and Vulnerabilities

We track threats, risks, and vulnerabilities so you don't have to.

Examples of current/ongoing cyber activity WaterISAC tracks:

- State-Sponsored Cyber Activity
- Phishing Campaigns
- CISA's Known Exploited Vulnerabilities (KEV)
- CISA's Industrial Control Systems Advisories (ICSAs)

State-sponsored Cyber Activity

“Why should I care about threats from state-sponsored actors?”

- They can and desire to disrupt critical infrastructure and/or sow doubt/distrust about safety/security of critical services.
- Less about the “who” (Russia, China, Iran) and more about the “what” – *behaviors/capabilities* – to defend against.

People's Republic of China (PRC) “Volt Typhoon”

- Confirmed actions against water and wastewater sector assets
- Living-off-the-Land (LOTL) techniques to hide in plain sight
- Pre-positioning on IT networks to enable disruption of OT



Disrupted **Volt Typhoon** Botnet and Testimony on Preeminent Cyber Threat Posed by the PRC

FEB 01, 2024 IN CYBERSECURITY, OT-ICS SECURITY



(TLP:CLEAR) WaterISAC Advisory – PRC-sponsored **Volt Typhoon** Activity and Supplemental Living Off the Land Guidance

FEB 08, 2024 IN CYBERSECURITY, OT-ICS SECURITY, FEDERAL & STATE RESOURCES

Reported Cyber Attacks On U.S. Critical Infrastructure (Source: ODNI)

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024

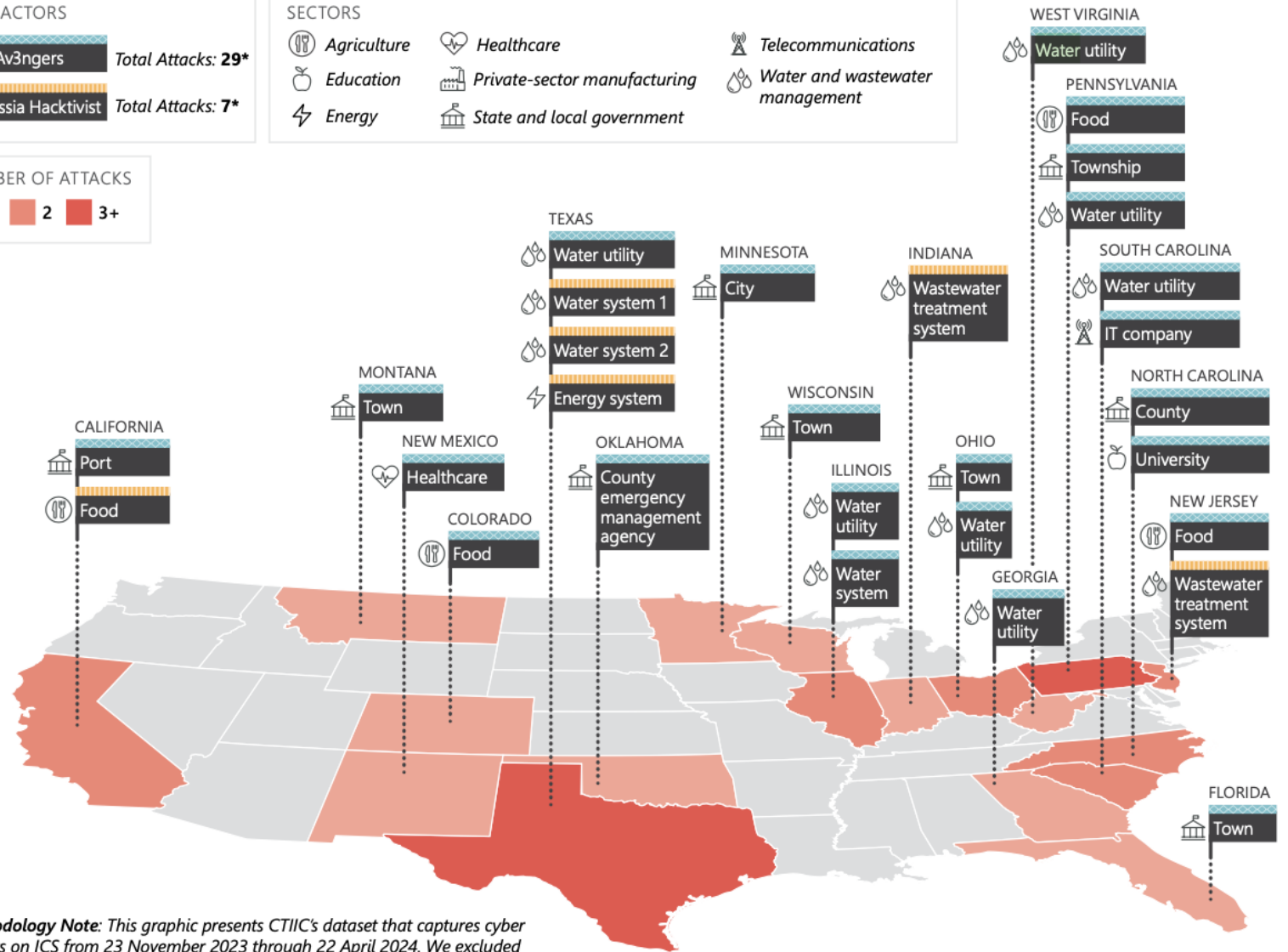
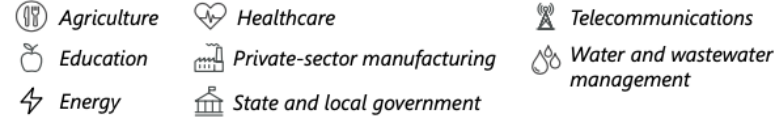
CYBER ACTORS



NUMBER OF ATTACKS



SECTORS



Methodology Note: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.

*Including seven attacks at additional US locations.

Phishing Campaigns – Maine CDC Impersonation

WaterISAC Advisories on state agency impersonations:

- January 2024 | Phishing Campaign Impersonates State CDC Drinking Water Program (Maine)
- June 2024 | Another Phishing Campaign Impersonates *the same* State CDC Drinking Water Program (Maine)


Maine Phishing Impersonation Examples

January 2024

June 2024

Screenshot of Attempted Phishing Email:

Division of Environmental and Community Health External



Division of Environmental and Community Health
LICENSED OPERATORS INFORMATION UPDATE.

Dear [REDACTED]

Note: This secure verification link below will expire after 24 hours, and if we did not receive your verification / update before the link expire, we will have to revoke your license.


Expiration Date	[REDACTED]
License ID	[REDACTED]
Last Name	[REDACTED]
First Name	[REDACTED]
Address	[REDACTED]
City	[REDACTED]
State	[REDACTED]
Zip	[REDACTED]
Email	[REDACTED]
Phone	[REDACTED]
Distribution	[REDACTED]
Treatment	[REDACTED]
County	[REDACTED]

[CLICK HERE TO VERIFY OR UPDATE YOUR INFORMATION.](#)

NOTICE - This communication may contain confidential and privileged information that is for the sole use of the intended recipient. Any viewing, copying, or distribution of or reliance on this message by unintended recipients is strictly prohibited. If you have received this message in error, please notify us immediately by replying to the message and deleting it from your computer.

DWP Comment: Cyber attacker used the Maine.gov logo and Division title in the email subject line and header to give the phishing email the appearance of legitimacy.

DWP Comment: Cyber attacker prompted recipient to click links in the phishing email. Hover your mouse over the hyperlink (**do not click!**) to show you the real web address the link will send you to.



2024 Maine Gov Information Verification.

Dear [REDACTED]


Kindly confirm if the below information about you is correct and up to date. This is a final awareness for information verification.

This secure verification link below will expire after 24 hours. We will have to revoke your license if we do not receive your verification/update before the link expires.

Expiration Date	[REDACTED]
License #	[REDACTED]
FIRST_NAME_TEXT	[REDACTED]
LAST_NAME	[REDACTED]
Address	[REDACTED]
City	[REDACTED]
State	[REDACTED]
Zip	[REDACTED]
E-mail	[REDACTED]
Phone	[REDACTED]
Driller Grade	[REDACTED]
Installer Grade	[REDACTED]

[CLICK HERE TO CONFIRM OR VERIFY YOUR INFORMATION.](#)

This provided is informational, confidential, and privileged, and is not to provide legal advice. Unless you are the intended addressee (or authorized to receive for the intended) you may not use, copy, disclose, or forward the message or any information contained in the message without the sender's permission. If you have received this message in error, please advise the sender by reply email and delete the message.

 2024

Cyber Vulnerabilities

Patching is hard, exploiting unpatched devices...not so much!

Vulnerability information sources WaterISAC tracks:

- CISA's Known Exploited Vulnerabilities (KEV) Catalog
- CISA's Industrial Control Systems Advisories (ICSAs)

For both OT/IT: update or patch as you are able, compensate with other controls when you can't patch, isolate when neither is possible.

12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Download the guide: www.waterisac.org/fundamentals

2024



12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks

1. Incident Response Planning
2. Minimize Control System Exposure
3. Cybersecurity Culture
4. Threat Detection & Monitoring
5. Understanding Assets
6. Enforce Access Controls
7. *Physical Access Protection*
8. *Cyber-Physical Safety Systems*
9. *Vulnerability Management*
10. Governance
11. Third Party Risks
12. Information Sharing



Cyber Resilience Resources

WaterISAC

- [Cybersecurity Fundamentals for Water and Wastewater Utilities](#)
- [WaterISAC Monthly Cyber Resilience Briefings](#)
- [WaterISAC Champions](#)

Federal (CISA, EPA, FBI, etc.)

- [Top Cyber Actions for Securing Water Systems](#)
- [Water and Wastewater Sector - Incident Response Guide](#)
- [CISA's Free Cyber Vulnerability Scanning for Water Utilities](#)
- Visit CISA's page on [Water and Wastewater Cybersecurity](#)
- [CISA's Cross-Sector Cybersecurity Performance Goals \(CPGs\)](#)
- [Security Advisors](#) (including Cybersecurity Advisors – CSA's)

Other

- [Cyber Readiness Institute \(CRI\) Cyber Readiness Program - Resiliency for Water Utilities Program](#)
- [Five ICS Cybersecurity Critical Controls](#)
- [Protecting Critical Water Systems with the Five ICS Cybersecurity Critical Controls](#)
- [Top 20 Secure PLC Coding Practices](#)
- [Dragos OT-CERT](#)

American Water Works Association (AWWA) Cybersecurity & Guidance

- [Water Sector Cybersecurity Risk Management Guidance](#)
- [Assessment Tool](#)
- [Small Systems Guidance](#)



Physical Security Threat Landscape

- The Water and Wastewater Sector faces a heightened threat of being targeted by a wide range of threat actors.
- Terrorists and violent extremists represent a particularly dangerous threat given their perception of critical infrastructure as a viable and attractive target.
- Common criminals continue to represent an enduring threat to the Water and Wastewater Sector, committing most of the incidents.



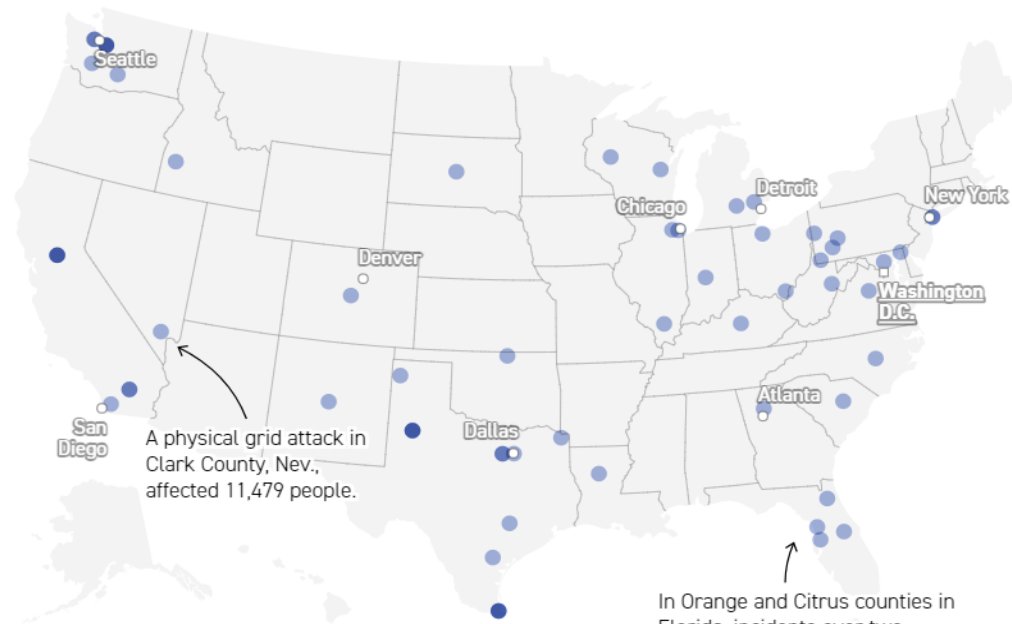
Source: Stimson Center



Physical Security Incidents Affecting the Power Grid

Electric grid under assault

60 physical attacks or threats reported from January through March (most recent data available). Darker circles indicate multiple incidents.



Note: Some locations are approximate based on available data.

Source: DOE

Catherine Morehouse/POLITICO



Physical Threat Actors

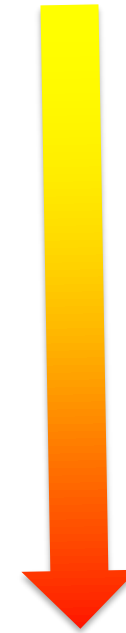
- Common criminals
 - Theft
 - Minor sabotage/tampering
- Insider Threat/Workplace violence
 - Threat
 - Assault
- Terrorists/Extremists
 - Assault
 - Sabotage/tampering
 - Contamination
- Hostile Nation States
 - Sabotage/tampering
 - Contamination

High
Probability

Low
Consequence

Low
Probability

High
Consequence



Notable Terrorist/Extremist Plots and Incidents Involving the Sector

- November 2023 | San Carlos, CA | An anarchist violent extremist who was inspired by the Middle East conflict and against U.S. support for Israel, sabotaged water distribution infrastructure.
- November 2021 | Greenbelt, MD | Two members of the neo-Nazi group "The Base" were sentenced to nine years in prison for planning to poison water supplies and engage in other terrorist activities.
- June 2021 | Unknown | Domestic violent extremists shot at a purported water treatment plant in a video.
- June 2018 | Cudahy, WI | An Islamic State supporter used a pro-Islamic State social media account to encourage a suspected Islamic State follower to poison water reservoirs with ricin.
- February 2014 | Cartersville, GA | Plot by militia members to trigger violent conflict against the government by attacking water utilities.



Insider Threats and Hostile Nation States

- Insider threats remain persisting threats to the sector and could potentially become a growing concern for critical infrastructure organizations going forward.
- Hostile nation states pose an increasing physical security threat to critical infrastructure operations due to the changing geopolitical landscape.



Top Actions to Enhance Your Physical Security

1. Join an information sharing community
2. Conduct a facility risk assessment
3. Document emergency response plans, policies, and procedures
4. Conduct awareness training of the threats and risk facing the sector
5. Exercise emergency response plans and other security contingencies
6. Network with neighboring utilities and local law enforcement

MEMBER PORTAL

- [Detailed FAQs](#)
- [Resource Center](#)
- [Webcast Archive](#)
- [Upcoming Events](#)

UPCOMING EVENTS

- Water Sector Cyber Resilience Briefing
 - 12 Cybersecurity Fundamentals for Water and Wastewater Utilities
Wrap-up
 - Wednesday, December 18 at 2 PM ET

THANK YOU!

Tom Dobbins

Executive Director
dobbins@waterisac.org

Scott Biernat

Manager, Accounts
biernat@waterisac.org

Eugenia Cadena

Manager, Administration
cadena@waterisac.org

Alec Davison

Lead Analyst
davison@waterisac.org

Mayya Saab

Managing Director
saab@waterisac.org

Dan Hartnett

AMWA Chief Policy Officer
Hartnett@amwa.net

Andrew Hildick-Smith

OT Security Lead
hildick-smith@waterisac.org

Tracy Kinney

Director of Marketing and Events
kinney@waterisac.org

Jennifer Lyn Walker

Infrastructure Cyber Defense Director
walker@waterisac.org

April Zupan

All-Hazards Risk Analyst
zupan@waterisac.org

April Zupan

Deputy Project Manager
zupan@waterisac.org

WWW.WATERISAC.ORG

FOLLOW US ON

