# INFORMATIONAL WEBINAR

*Getting to Know WaterISAC*

June 11, 2025

# 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.

WATER ISAC

# HOW IT WORKS


WATER ISAC

# 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.

## NEWSLETTERS

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

## ANALYSIS

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

## RESOURCES

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

WATER ISAC

# 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
- H2OEx – In-person, single-day learning and exercise event
  - Daytona, FL - July 28
  - Los Angeles, CA - Sept 11
  - Arlington, TX - Nov 6

WATER ISAC

# POLICY UPDATES

- Congressional Priorities
- Water Risk and Resilience Organization legislation
- Water Preparedness and Resilience legislation
- CISA Reauthorization

# POLICY UPDATES

**Congressional Cybersecurity Priorities**

- Consistently hearing that Congress must “do something” on water cybersecurity
- What that “something” is, is not clear
- Water-cyber provisions may be included in a water infrastructure reauthorization bill that Congress will begin to write later this year
- AMWA and others in the sector are working to put good ideas on the table ahead of these debates

WATER ISAC

# POLICY UPDATES

**Water Risk and Resilience Organization (WRRO) Establishment Act**

- Introduced in House of Representatives by Rep. Rick Crawford (R-Ark.) as H.R. 2594
- 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
- Based on the NERC model in the energy sector
- Working to line up a Senate sponsor

WATER ISAC

# POLICY UPDATES

**WaterISAC Threat Protection Act**

- Rep. Jan Schakowsky (D-Ill.) and Sen. Ed Markey (D-Mass.) reintroduced in March as H.R. 1118/S. 2344
- Would direct EPA to do more to promote WaterISAC to water and wastewater systems, and authorize funds to offset membership dues
- Would authorize funds for EPA that could be used to help water systems gain or maintain WaterISAC memberships
- Based on a DOE program authorized in 2021

# POLICY UPDATES

**Cybersecurity Information Sharing Act of 2015 Reauthorization**

- 2015 law provided a ten-year authorization governing cyber threat information sharing practices among and between federal government and sector partners.
- Current law provides critical liability protections for entities that share cyber incident info with the federal government. Reauthorization bill would continue these.
- 50+ organization stakeholder letter called on Congress to reauthorize CISA prior to expiration in September 2025. DHS Secretary Noem endorsed reauthorization in recent congressional testimony
- Stakeholders pushing Congress to act prior to expiration

WATER ISAC

# THANK YOU!


## Dan Hartnett

Chief Policy Officer

Association of Metropolitan Water Agencies

Hartnett@amwa.net

# 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)

WATER ISAC

# 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.

WATER ISAC

# State-Sponsored Cyber Threats (The Main Ones)

- People's Republic of China-Affiliated Threat Actors
- Pro-Russia Hacktivists
- Iranian Government Islamic Revolutionary Guard Corps (IRGC)-affiliated CyberAv3ngers
- North Korean (DPRK)-Affiliated Threat Actors

WATER ISAC

# 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

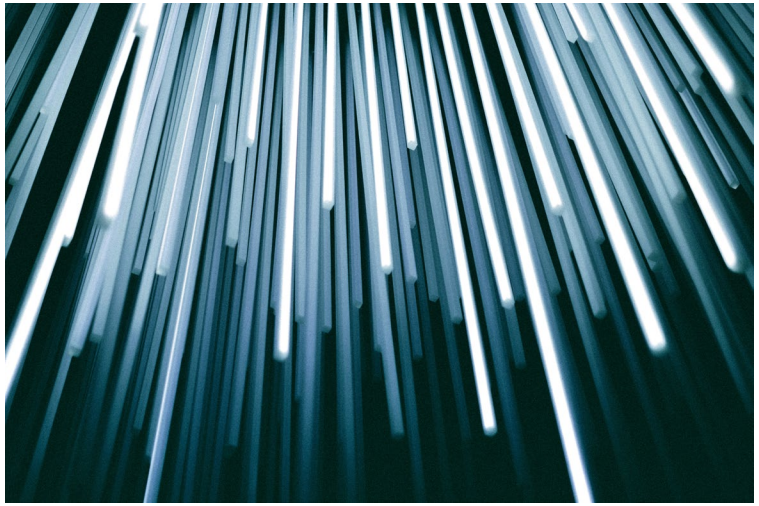
FEB 08, 2024 IN CYBERSECURITY, OT-ICS SECURITY, FEDERAL & STATE RESOURCES

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

WATER ISAC

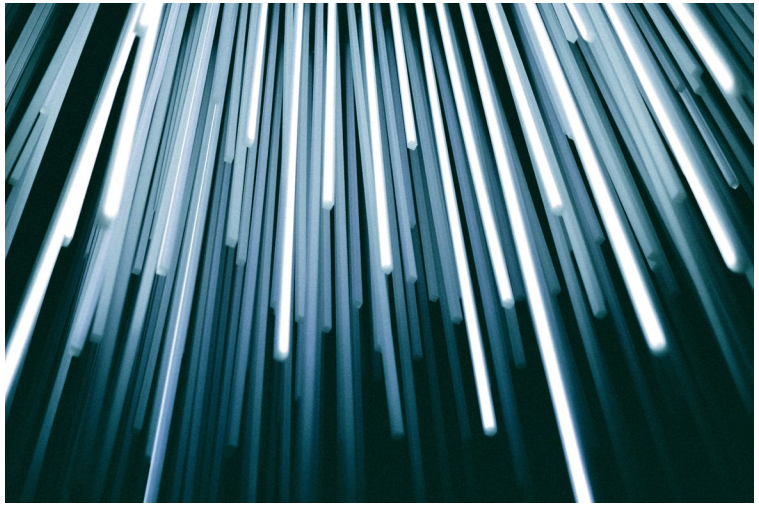
# Salt Typhoon

- Compromised at least 9 telecommunication companies including major ISPs AT&T, Verizon, and Lumen Technologies
- Appear to have access deep into the routing functions of major ISPs,
- Have the potential to impact OT



# Silk Typhoon

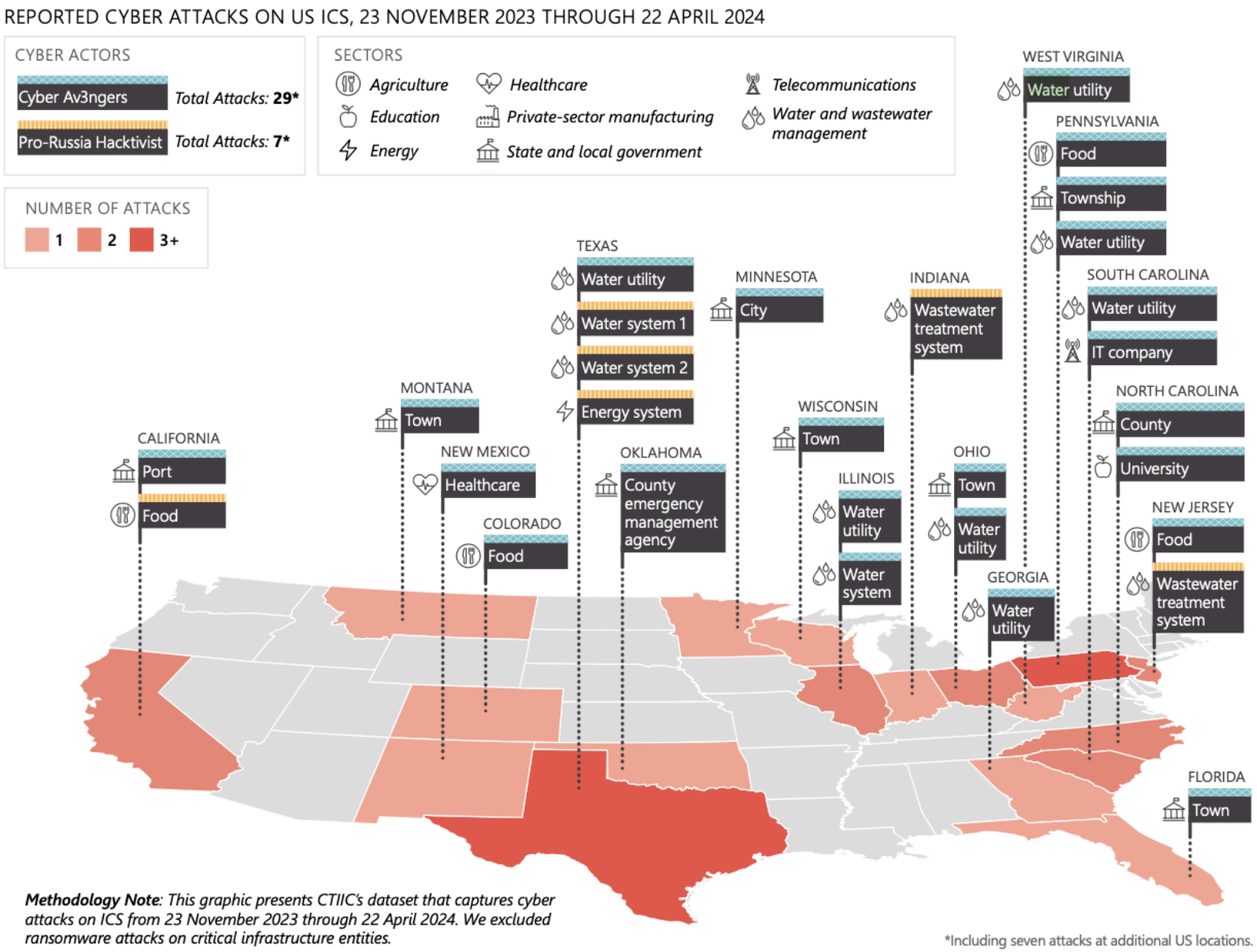
- Microsoft Threat Intelligence shared details of Silk Typhoon targeting remote management tools and cloud services in supply chain attacks giving them access to downstream customers.
- https://www.waterisac.org/portal/tlpclear-silk-typhoon-another-chinese-affiliated-threat-actor-targets-it-supply-chains



# Russian Hacktivist Claims to Have Gained Access to a Water Utility's OT Systems, Underscoring Importance of Cyber Hygiene

- (TLP:AMBER) Russian Hacktivist Claims to Have Gained Access to a Water Utility's OT Systems, Underscoring Importance of Cyber Hygiene

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



# WaterISAC Advisories

**(TLP:AMBER) WaterISAC Advisory – WWS Billing Software Impacted by Ransomware Group**

- June 9, 2025 | https://www.waterisac.org/portal/tlpamber-waterisac-advisory-%E2%80%93-wws-billing-software-impacted-ransomware-group

# Maine Phishing Impersonation Examples

**Screenshot of Attempted Phishing Email:**

## January 2024

Division of Environmental and Community Health External

Maine.gov

**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 | |
| License ID | |
| Last Name | |
| First Name | |
| Address | |
| City | |
| State | |
| Zip | |
| Email | |
| Phone | |
| Distribution | |
| Treatment | |
| County | |

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.

## June 2024

Maine.gov

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 | |
| License # | |
| FIRST_NAME_TEXT | |
| LAST_NAME | |
| Address | |
| City | |
| State | |
| Zip | |
| E-mail | |
| Phone | |
| Driller Grade | |
| Installer Grade | |

CLICK HERE TO CONFIRM OR VERIFY YOUR INFORMATION.

n 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 u 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.*

WATER ISAC

# 12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Download the guide: **www.waterisac.org/fundamentals**

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

2024

WATER ISAC

**12 Cybersecurity Fundamentals for Water and Wastewater Utilities**

*Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks*

# 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

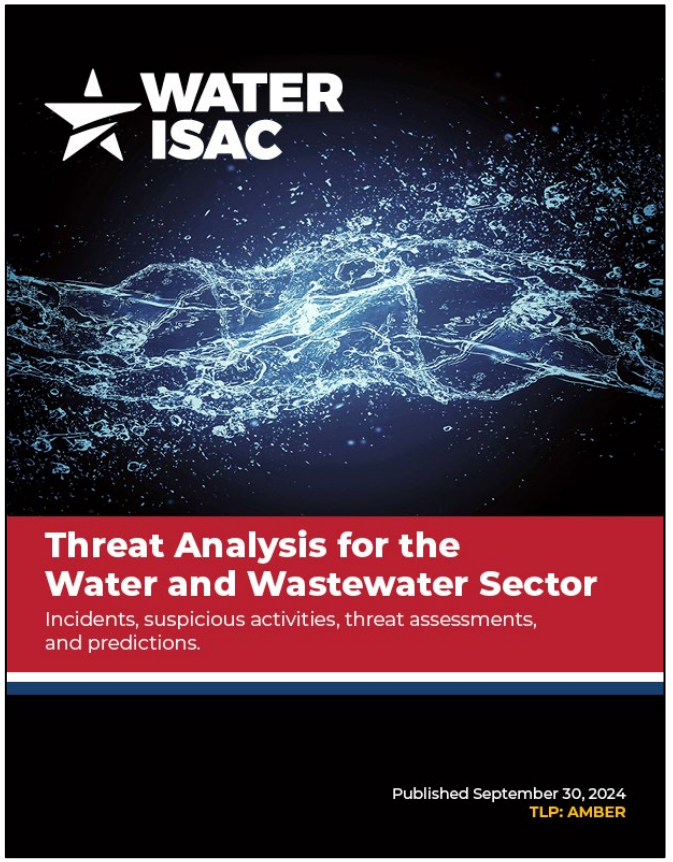
American Water Works Association (AWWA) Cybersecurity & Guidance

- Water Sector Cybersecurity Risk Management Guidance
- Assessment Tool
- Small Systems Guidance

WATER ISAC

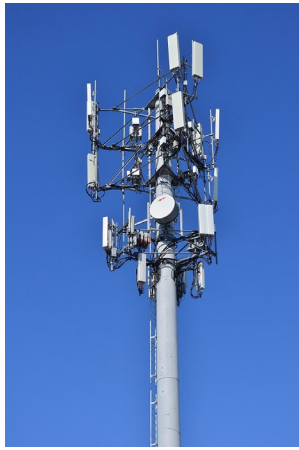
# Water Sector Physical Security Threat Landscape

- The physical security threat landscape facing the water and wastewater sector today is increasingly complex, dynamic, and volatile. Several domestic and international factors are driving a rise in threats to critical infrastructure
- 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.

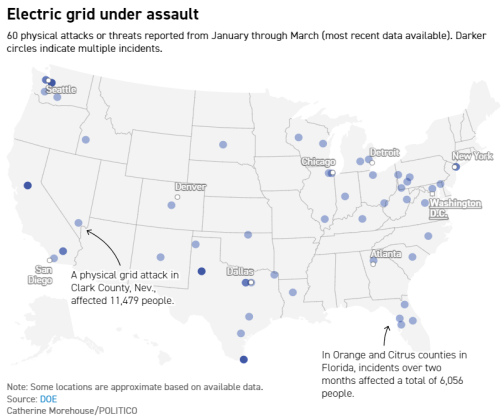



WATER ISAC

# Other Critical Infrastructure Physical Security Threat Landscape

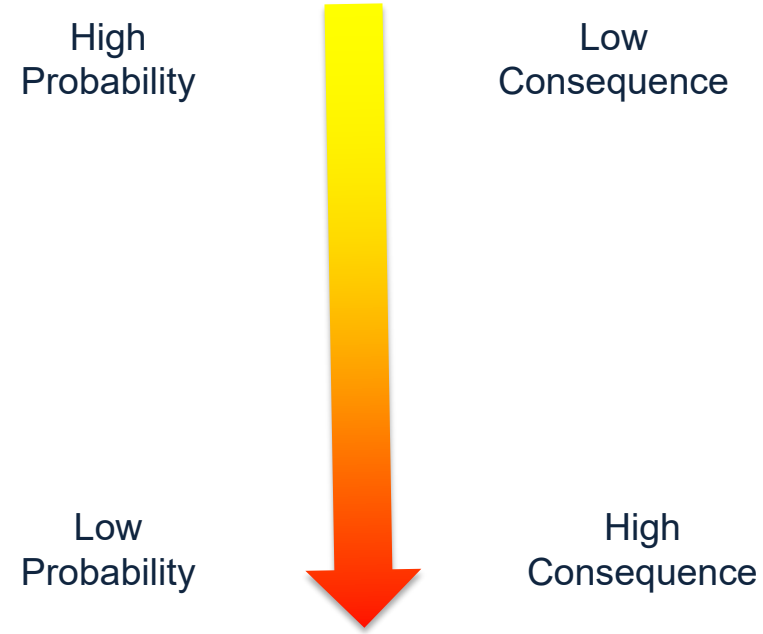


- The energy sector very likely remains the most targeted sector, with threats, plots, and attacks against electric infrastructure having significantly increased since at least 2019
- The communications sector also faces increasing physical security incidents. Criminals and other threat actors have targeted sector assets to steal valuable components and, in some cases, to disable communications for other malicious purposes
- The transportation sector faces a myriad of physical threats stemming from multiple types of threat actors



# 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




WATER ISAC

# 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.


WATER ISAC

# 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 – can't defend against what you don't know
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

WATER ISAC

# Key Takeaways

1. There is a growing number of physical security incidents at water and wastewater utilities that cause operational impacts
2. A widening range of physical threat actors increasingly perceive disruptive or destructive attacks on critical infrastructure as viable tactics to advance their malicious agenda
3. Conduct suspicious activity and threat awareness trainings with employees
4. Exercise responding to hostile events and disasters

WATER ISAC

# MEMBER PORTAL

- Detailed FAQs
- Resource Center
- Webcast Archive
- Upcoming Events

# UPCOMING EVENTS

- Water Sector Cyber Resilience Briefing
  - Wednesday, June 25 at 2 PM ET
- Water Sector Physical Security Threat Briefing
  - Wednesday, July 9 at 2 PM ET
- H2OEx – In-person, single-day learning and exercise event
  - Mon July 28 - Daytona Beach, FL
  - Thurs Sept 11- Los Angeles, CA
  - Thurs Nov 6 - Arlington, TX

WATER ISAC

# 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

**Chase Snow**
Cyber Threat Analyst
snow@waterisac.org

**Tracy Kinney**
Director of Marketing and Events
kinney@waterisac.org

**Jennifer Lyn Walker**
Infrastructure Cyber Defense Director
walker@waterisac.org

**April Zupan**
Deputy Project Manager
zupan@waterisac.org


**WWW.WATERISAC.ORG**

**FOLLOW US ON** in

WATER ISAC