

Building Security and Resilience to Cyber Threats, Disinformation and other Hazards in the Water and Wastewater Sector

October 7, 2020



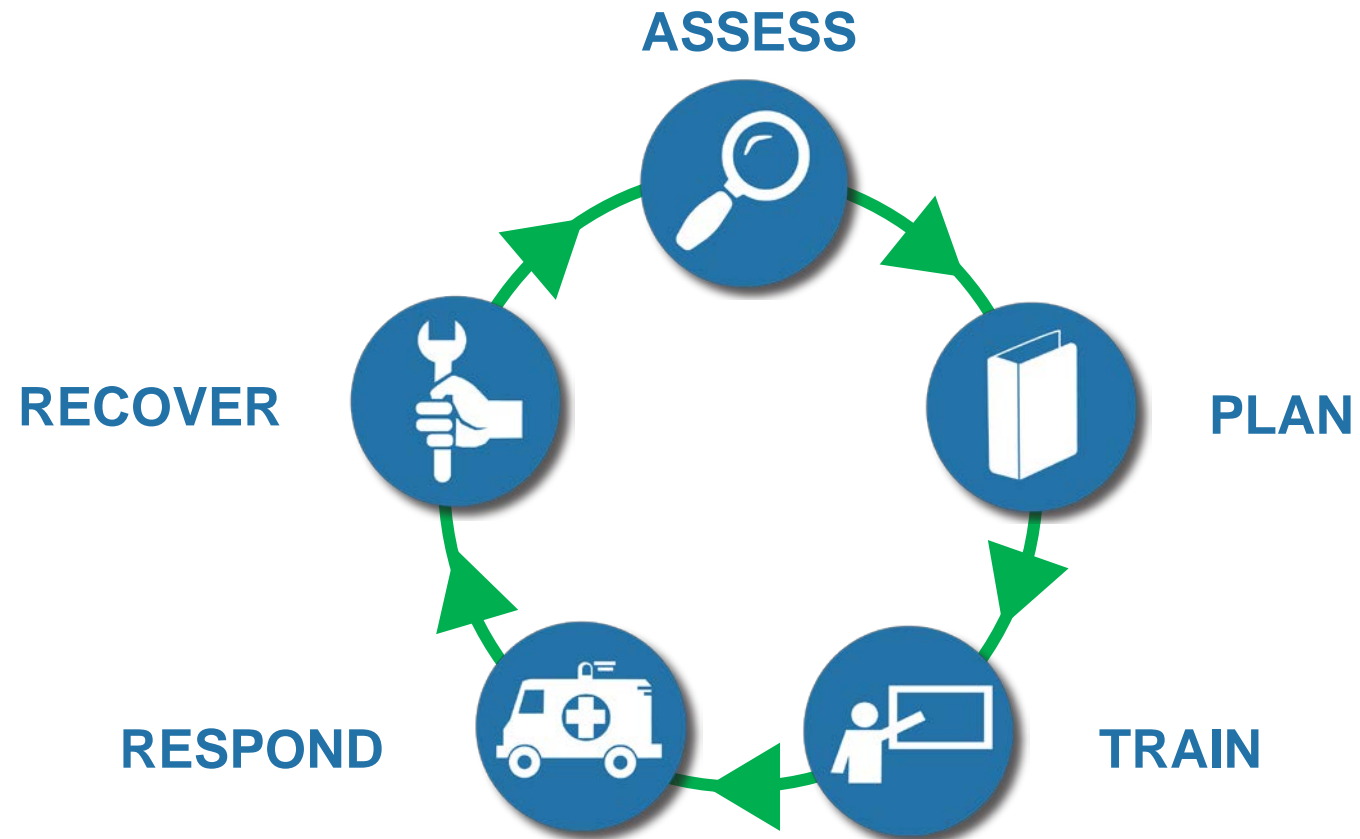
How to Participate

- Interactions
 - Ask questions in the Questions/Chat box.
 - Polling questions.
- Troubleshooting
 - For help, contact wsdwebinarsupport@cadmusgroup.com or call 1(617) 673-7018.
- Tips
 - At the end of the webinar, please complete the webinar evaluation.
 - A PDF of the slides, a webinar recording, and other relevant materials will be sent after the webinar.

EPA is the Sector-Specific Agency for Water



Water Resilience Framework



Today's Webinar Presenters



Nelson Mix

Captain, U.S. Public Health Service

Office of Water, Water Security Division

U.S. Environmental Protection Agency



Chuck Egli

Lead Analyst

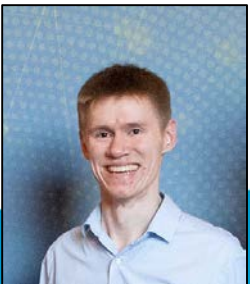
WaterISAC



Jennifer Lyn Walker

Cyber Threat Analyst

WaterISAC



Mikko McFeely

Manager of Resilience and Sustainability Affairs

Association of Metropolitan Water Agencies



Cybersecurity for the Water Sector



Presentation Topics:

1. Water Sector Cyber Security Overview
2. Cybersecurity for Water Quality Surveillance and Response Systems (SRSs)
3. Recap





Cyber Threats to Water Utilities

- Many water utilities across the United States are being victimized by cyber-attacks
- Both large urban and small rural utilities have suffered disabling cyber incidents
 - Recovery costs can be high
- Basic cyber security practices can prevent many cyber attacks
- Robust preparation, response, and recovery planning can greatly reduce the impact of a successful cyber-attack



Many Methods of Cyber Attack

- Any network that can be accessed through the Internet or by remote access is vulnerable
- Examples of cyber-attack vectors
 - Phishing attacks that plant malware or steal credentials
 - Pirated wireless communications
 - Compromised third-party networks or services
 - Corrupted personal devices of employees or contractors with remote access to utility networks
 - Web sites with corrupted content
 - Insider attacks

What Should Water Utilities Do?

1. **Build** cybersecurity best practices into utility operations



2. **Prepare** for a cyber attack, including the loss of process control, data, and communications systems

Building Cybersecurity into Utility Operations

1) Start with basic guidance. For example:

- [DHS CISA *Cyber Essentials*](#),
- [WaterISAC *15 Cybersecurity Fundamentals*](#)
- [EPA *Water Sector Cybersecurity Brief for States*](#)

2) Identify cyber gaps/vulnerabilities and develop actionable planning to reduce risk

• Examples of resources:

- [CISA *Cyber Resource Hub*](#)
- [EPA Technical Assistance Provider program](#)
- [AWWA *Process Control System Security Guidance*](#)
- [NIST *Cybersecurity Framework*](#)

Note: Many public and private sector resources are available



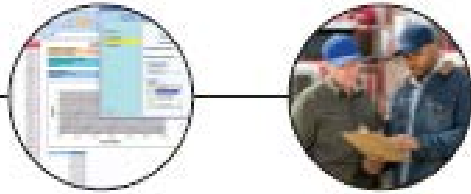
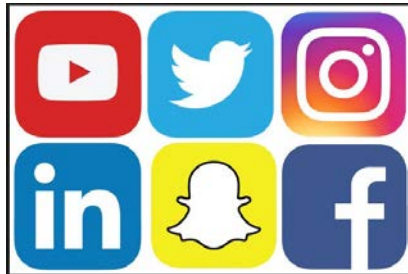
Preparing for a Cyber Attack

- Identify how to report a cyber incident and request help with response; include law enforcement, mutual aid programs and DHS
 - Report incident to DHS National Cybersecurity and Communications Integration Center (NCCIC): 888-282-0870 or NCCIC@hq.dhs.gov
- Update the utility ERP for a cyber incident
 - Include the failure of process control, business administration, and communications systems
 - **Planning, training, and drilling** for preparation, response, and recovery are critical
- Resource: [EPA Cyber Incident Action Checklist](#)

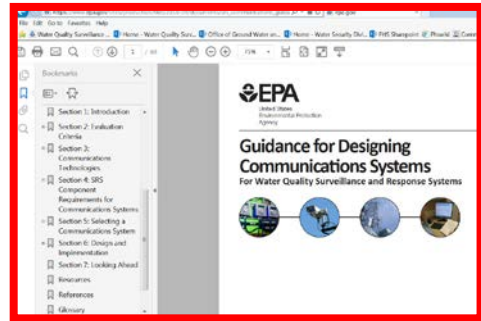
Preparing for a Cyber Attack

- **Train** essential personnel to perform mission critical functions if a cyber incident disables business, process control and communications systems
 - Include the manual operation of water collection, storage, treatment and conveyance systems
- **Conduct drills and exercises** for responding to a cyber incident that disables critical business, process control and communications systems
- Set up an automatic **back-up on critical systems** and ensure the process is producing a readable, uncorrupted restore file on a routine basis

Topic 2: Cybersecurity for a Water Quality Surveillance and Response System



Social Media Monitoring

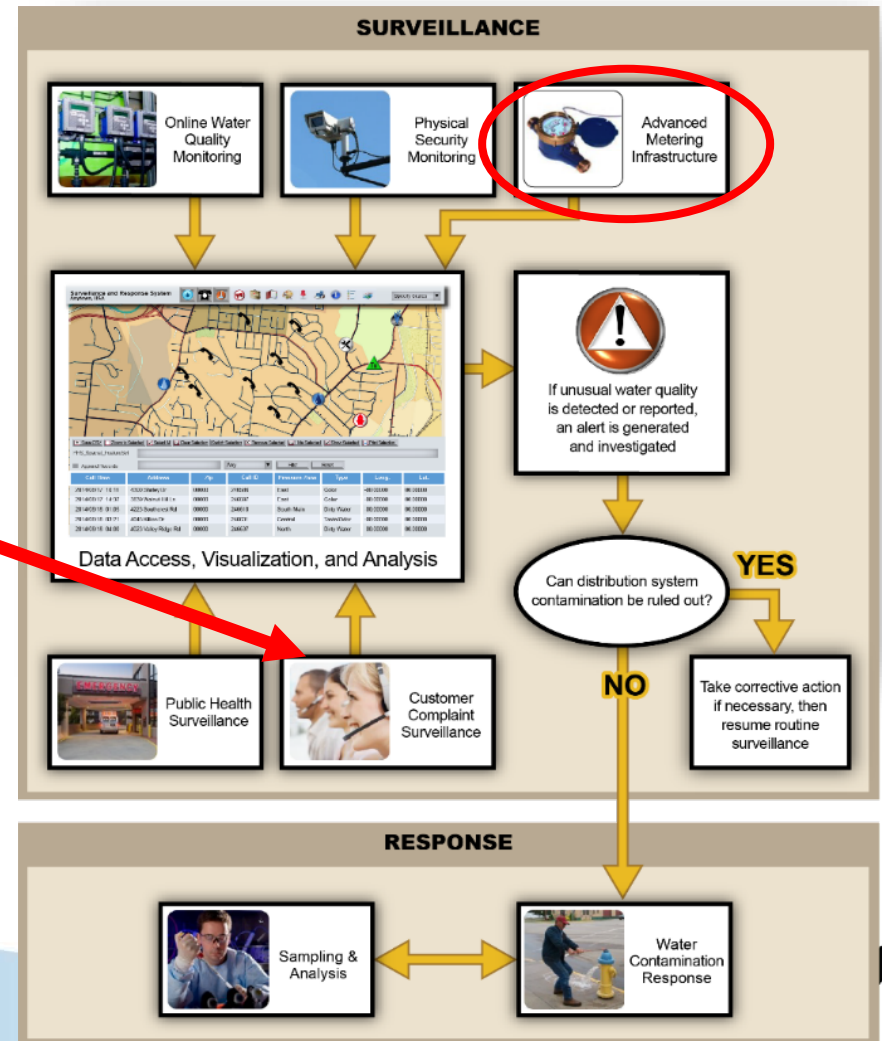


COMPLAINTS SUBMITTED BY CUSTOMER



PHONE
EMAIL
WEB FORMS

INSTANT MESSAGES
TEXT MESSAGES
SOCIAL MEDIA



Communications

Wired Technologies:

- POTS
- DSL
- T1
- Frame Relay
- MPLS
- TLS
- Utility-owned fiber optic

Wireless Technologies:

- Digital Cellular
- Utility-owned wireless

Other considerations: Customer Complaint Surveillance, IoT, 5G, LoRa, CAT M1, etc

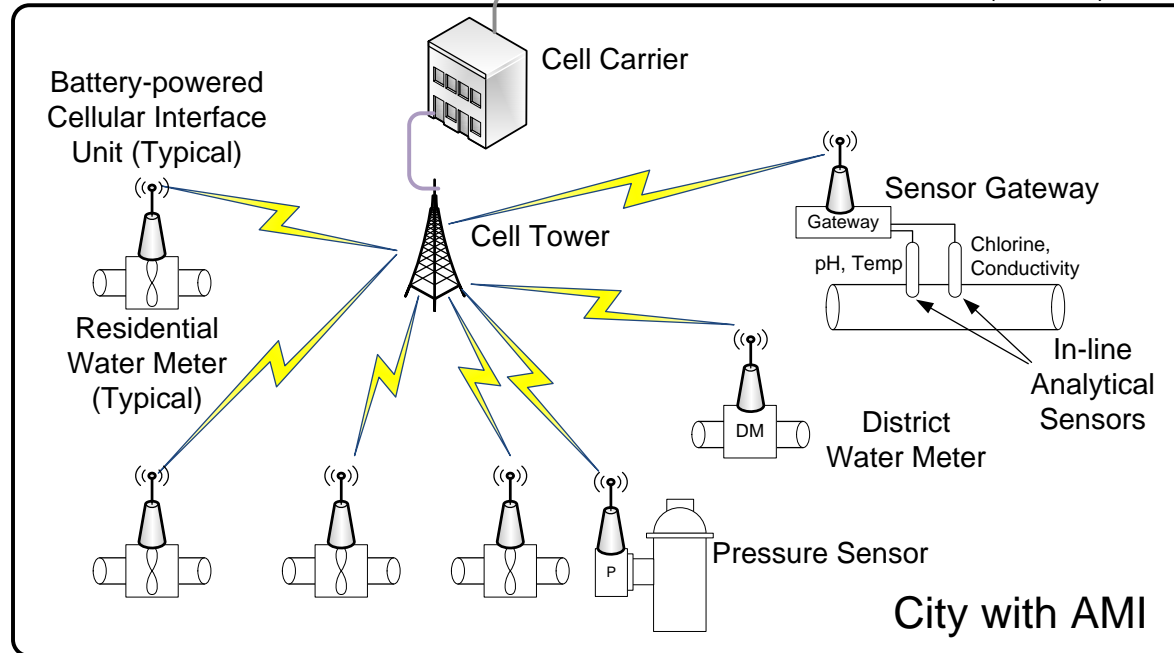
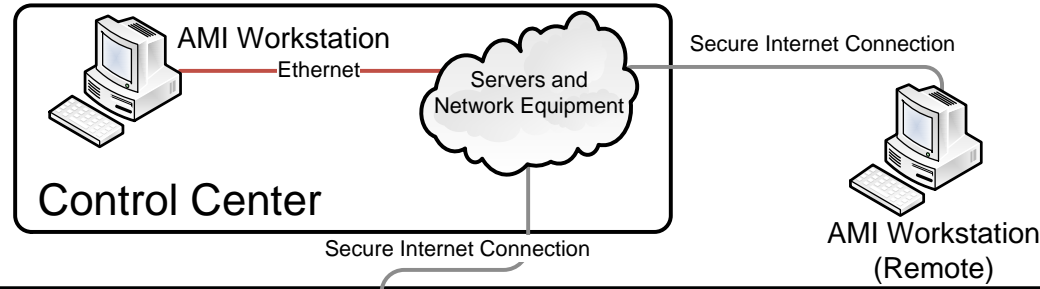
Table 3-1. Commonly Available Communications Technologies

Communication Technology	Extent of Use	Data Tr. Rate	Security	Reliability	Distance	Installation Cost	Provider Fees	Maintenance
Plain Old Telephone System (POTS): POTS is the basic form of wired voice communication. A conventional modem can be used over POTS for data communication, but is limited to 56 kilobits per second without data compression.	○	○	●	●	●	●	●	●
Digital Subscriber Line (DSL): DSL uses existing POTS infrastructure for data transmission between facilities via the Internet, although some providers offer a private network option at additional cost. DSL is capable of transmission rates of up to 5,000 kilobits per second to the end user and up to 768 kilobits per second from the end user.	●	●	○	●	●	●	●	●
T-Carrier 1 (T1) Line: A T1 line is a dedicated point-to-point data connection between facilities that is capable of transmission rates up to 1.54 megabits per second.	●	●	●	●	●	○	○	●
Frame Relay: To the end user, frame relay appears to be a dedicated point-to-point data connection up to 1.5 megabits per second, similar to a T1 line. However, providers vary the size and routing of frame relay data packets to optimize usage of their infrastructure, resulting in a reduction in costs relative to that of T1 lines.	●	●	●	●	●	○	●	●
Multi-Protocol Label Switching (MPLS): This newer technology is replacing T1 and frame relay connections and capable of transmission rates up to 622 megabits per second	●	●	●	●	●	●	●	●
Transparent LAN Service (TLS): Also called "Metro Ethernet," TLS is an emerging technology that provides an Ethernet data transmission rate connections between facilities of 10, 100, or 1000 megabits per second.	●	●	●	●	●	●	●	●
Utility-Owned Fiber Optic: This dedicated point-to-point data connection between facilities is capable of transmission rates up to 10 gigabits per second.	●	●	●	●	●	○	●	○
Digital Cellular: Digital cellular uses wireless transceivers to connect to a provider's cellular network for data transmission. The cellular technologies, third generation (3G) and fourth generation (4G), have transmission rates of up to 800 kilobits per second and 10 megabits per second, respectively. Upload and download data transmission rates are often asymmetric with upload rates being lower.	●	●	●	●	●	●	●	●
Utility-Owned Wireless: Utility-owned wireless uses utility equipment and infrastructure for data transmission over unlicensed or licensed frequency bands. Transmission rates vary widely depending on the modulation technology and frequency band (9.6 kilobits per second for low-speed, narrowband technologies and up to 7 gigabits per second for high-speed Wi-Fi). This category also includes microwave technologies.	●	●	●	●	●	○	●	○

Attribute Key: ● Strong ● Moderate ○ Weak

Advanced Metering Infrastructure

example communications architecture



Identify

Protect

Detect

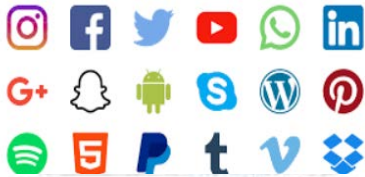
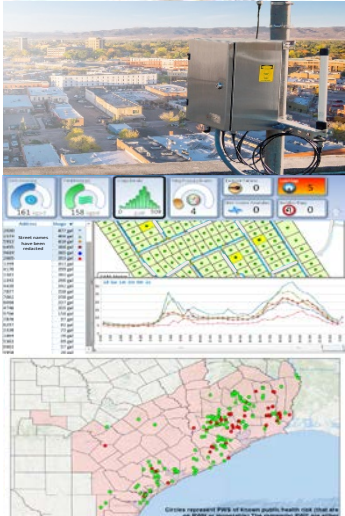
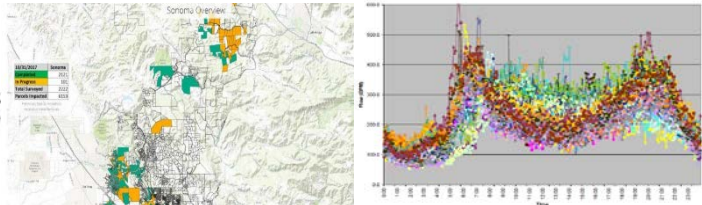
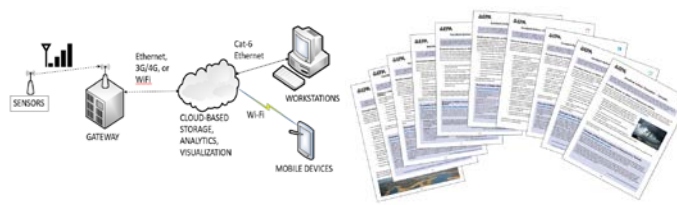
Respond

Recover

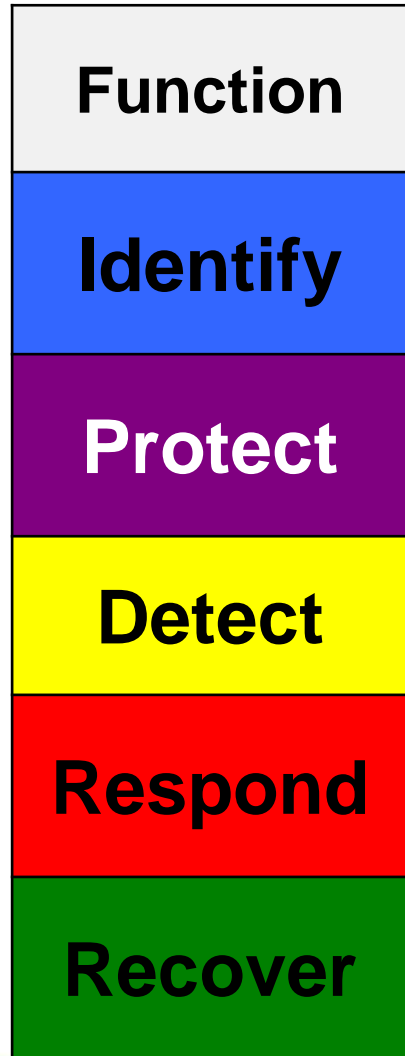




Topic 3: Recap

Recap – WQSRS and Comms



Water Contamination Response

Recap – Key Messages



Commit to cybersecurity



Start with the **basics**



Prepare to respond



Water Information Sharing and Analysis Center

Overview
- and -
Cyber Incidents and Threat Activity against Water Utilities

October 7, 2020

Mission

To enhance the security of water and wastewater utilities by providing information and tools for preventing, detecting, responding to, and recovering from all hazards.

Areas of Focus

- **Cybersecurity**
 - Business/Enterprise System
 - Industrial Control System
- **Physical Security**
 - Terrorism and Extremism
 - Other Malicious Activity
- **Natural Disasters**
- **Public Health and Other Hazards**

Background

- Established in 2002 at the urging of the White House, FBI, and EPA
- Created by the water and wastewater sector
- Focused solely on the sector's security needs
- Dues-based, non-profit
- The official security information sharing arm of the Water Sector Coordinating Council
- Board members: Utility managers and state primacy agency administrator

Supporting Organizations



Partnerships and Sources

- Federal agencies
 - EPA Water Security Division
 - Department of Homeland Security
 - FBI and InfraGard
 - FEMA, DOE, CDC, NOAA
- Other ISACs
- SMEs, private consultants, think tanks, researchers
- State primacy, law enforcement, and homeland security agencies

Information Gathering, Curation, and Analysis & Dissemination



Information Gathering

Federal

DHS, FBI, US EPA
FEMA, CDC, NOAA

State/Local

Law Enforcement
Homeland Security
Fusion Centers

Cross-Sector

Other ISACs
Other Sectors

Private

Research Orgs
Security Firms
Public Sources
Media



Threat analyses

Sodinokibi Ransomware Actors Adopt New Tactics

"Zerologon" – The Sky isn't Falling, but Your Domain Controller Could Be

Mitigation strategies

Selecting Secure Multi-factor Authentication Solutions

Best practices and guides

Recommended

**Cybersecurity
Practices**

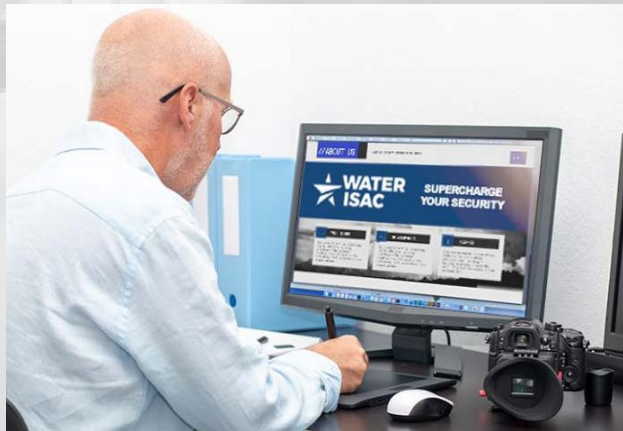
for Industrial
Control Systems

COVID-19 CHALLENGES AND
LESSONS LEARNED

Information Gathering – Member Reporting

Single report

- Online Incident Reporting Form: <https://www.waterisac.org/report-incident>
- Email: analyst@waterisac.org
- Phone: (866)H2O-ISAC



Quarterly Survey

- Conducted via Survey Monkey

CYBERSECURITY INCIDENTS

Provide information on cybersecurity incidents against your utility between April 1 and June 30, 2020.

* 20. Did your organization experience any cybersecurity incidents that involved:

- A **successful** or **unsuccessful** attack involving its industrial control systems; or

- A **successful** or **unsuccessful but significant** attack involving its business/enterprise information systems? (Factors that could contribute to an unsuccessful attack being significant include that it was targeted, revealed previously unknown vulnerabilities, or was nearly successful.)

Yes

No

Only WaterISAC staff see member reports and survey responses. Plus, as a private organization, WaterISAC is not subject to public disclosure laws.

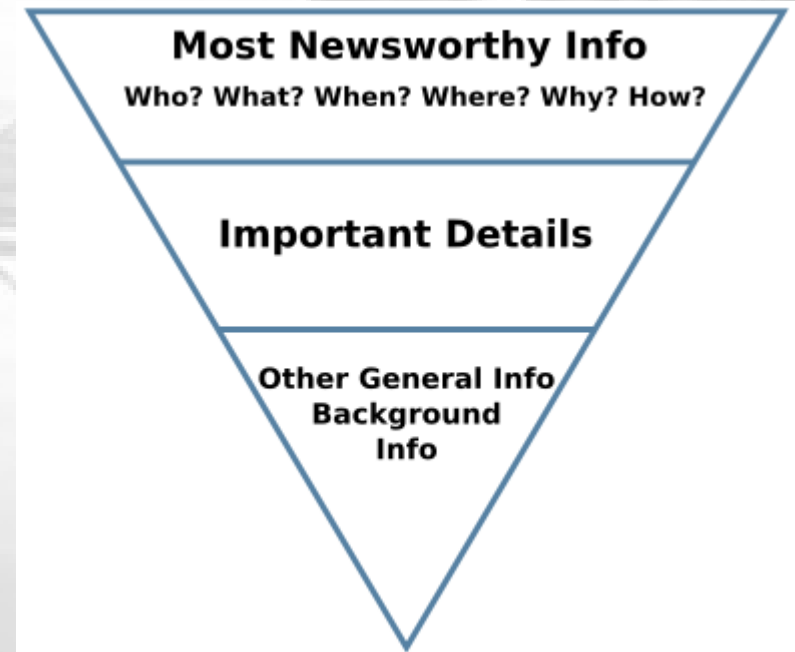
Curation

- Is this relevant to utilities?
- What is the priority of the information?
- What kind of information is it?
 - Current
 - Estimative
 - Research
 - Scientific and Technical



Analysis

- In House
- Consultation with SMEs
- Addresses:
 - What is it?
 - Why is it important?
 - What to do about it?
- Simplicity
- Objectivity



Dissemination

- Resource Center
- Security & Resilience Update
- Threat Advisories
- Threat and Incident Reports
- Guides
- Webcasts and Training

WaterISAC RESOURCE CENTER

AWIA Risk Assessments
and ERPs

COVID-19
Resources

Cybersecurity
Fundamentals

Perch Cyber Threat
Detection

Power Outage
Resilience

WaterISAC
Publications

Search

Filter by



Reset

Search tips

4550 total results

Sort by: **Date** Relevance Tiles List



Proactive Response and Recovery
for OT

SEP 22, 2020 IN CYBER SECURITY, RESILIENCE



Scammers Prey on Kindness during
Disasters

SEP 22, 2020 IN CYBER SECURITY



GE Reason S20 Ethernet Switch
(ICSA-20-266-02) – Products Used in
the Energy Sector

SEP 22, 2020 IN CYBER SECURITY

Security and Resilience Update

- Emailed 2x week
- Reporting and analysis on:
 - Cybersecurity
 - Physical Security
 - Resilience
 - Upcoming Events & Training

Security & Resilience Update

Stay current. Stay informed.
Stay alert.



July 21, 2020

In this issue:

SPOTLIGHT

- **TOMORROW - Water Sector Cyber Threat Web Briefing: Attack Surface Monitoring, A Security Must**

GENERAL SECURITY & RESILIENCE

- **IMPORTANT REMINDERS - Read WaterISAC's Latest Threat Analysis Report and Take the Security Incident Survey**
- **New CISA Exercise Kit for COVID-19 Recovery, and Other Pandemic Resources and Information**
- **New Value Analysis Guide and Brochure Help Agencies Evaluate Emergency Communications Cost Effectiveness**
- **The Challenges of Disrupting the Next American Terrorist Demand Vigilance by All**

CYBERSECURITY

- **Two More Attacks on Israeli Water Infrastructure – Israeli Government Advises Securing Cellular Communications Equipment**
- **Experiencing an Inbox Influx? – It's Probably Emotet, Again**
- **CISA Alert: Malicious Cyber Actor Use of Network Tunneling and Spoofing to Obfuscate Geolocation**
- **Vulnerability Advisory for Treck TCP/IP Stack**
- **Security Updates for Microsoft and Mozilla Products**

CYBERSECURITY

Two More Attacks on Israeli Water Infrastructure – Israeli Government Advises Securing Cellular Communications Equipment

Another round of cyber attacks reportedly targeted Israeli water infrastructure in June. According to officials, two cyber attacks took place. Reports state that one of the attacks hit agricultural water pumps in upper Galilee, while the other one hit water pumps in the central province of Mateh Yehuda. As reported to [Ynet News](#), “These are two spot and small sewage facilities in the agricultural sector that were repaired immediately and independently by the local person in charge of the kibbutz and the facility, without damage to service or actual impact,” the Water Authority said. Additionally, in what seems to be an exclusive, SecurityWeek learned the government advised organizations following the attacks in April to ensure their cellular communications equipment is not vulnerable, a point that has not been previously discussed. “An anonymous source with knowledge of the cyberattacks told SecurityWeek that both the latest and the April incidents involved vulnerable cellular routers, which enable organizations to remotely connect to their industrial systems.” In what is being called [a “tit-for-tat” between Israel and Iran](#), unsurprisingly neither side admits any wrongdoing for first or retaliatory attacks. [Read more about the recent attacks at SecurityWeek.](#)

Experiencing an Inbox Influx? – It’s Probably Emotet, Again

Last week, researchers observed Emotet awake from its 160 day slumber. The “public cyber enemy,” as Malwarebytes is calling it, seemed to warm-up as it began lightly populating inboxes on July 13. But by July 17, the malspam onslaught commenced with [nearly a quarter million messages](#). Emotet usually emerges out of hibernation with a new tactic in its arsenal, but so far nothing remarkable. It seems to be up to its old tricks, but that does not make it any less problematic as Emotet is used to spread additional malware, such as TrickBot and ransomware, including Ryuk. According to Proofpoint, the messages contain malicious Microsoft Word attachments or URLs linking to malicious Word documents hosted on compromised WordPress websites. In addition to frequent prior reporting and briefings on Emotet, Paul Scott, Director of Threat Research at Perch Security recently provided a comprehensive background for members during [WaterISAC’s Water Sector Cyber Threat Briefing on May 27](#). Additionally, members are encouraged to review the MITRE ATT&CK Framework to understand additional techniques used by [Emotet](#) for better network defense against this familiar foe. [Read more about Emotet’s awakening at Proofpoint](#)

Threat Advisories

Advisory: CISA and NSA Recommend Immediate Steps to Reduce OT and Control System Exposure amid Rising Tensions



**SUPERCHARGE
YOUR SECURITY**

WaterISAC Members:

The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) have published a joint alert recommending critical infrastructure owners and operators take immediate steps to reduce exposure of operational technology (OT) and control systems at this time of heightened geopolitical tensions. While not identifying specific nation states or recent events, the alert states that civilian infrastructure makes attractive targets for foreign powers attempting to do harm to U.S. interests or retaliate for perceived U.S. aggression.

[Access the alert at CISA.](#)

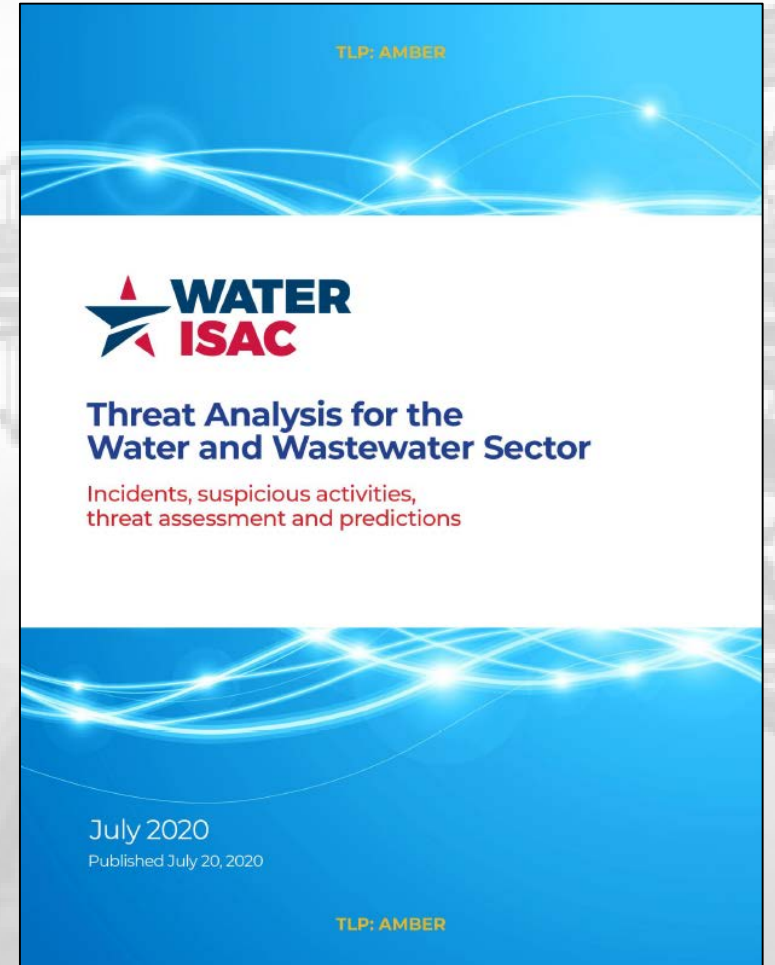
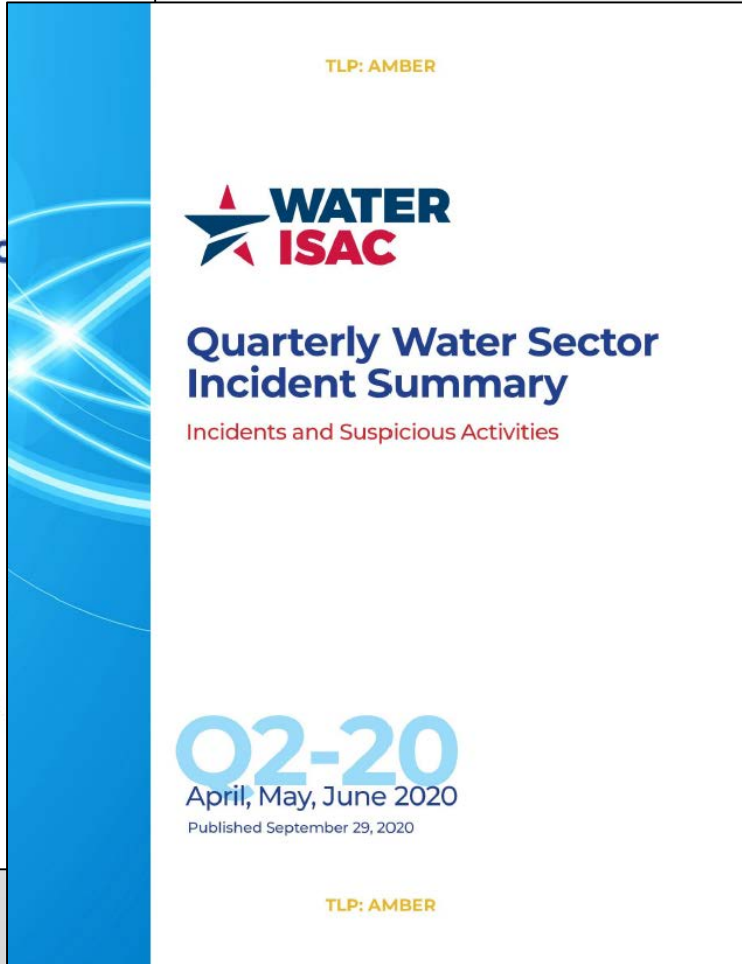
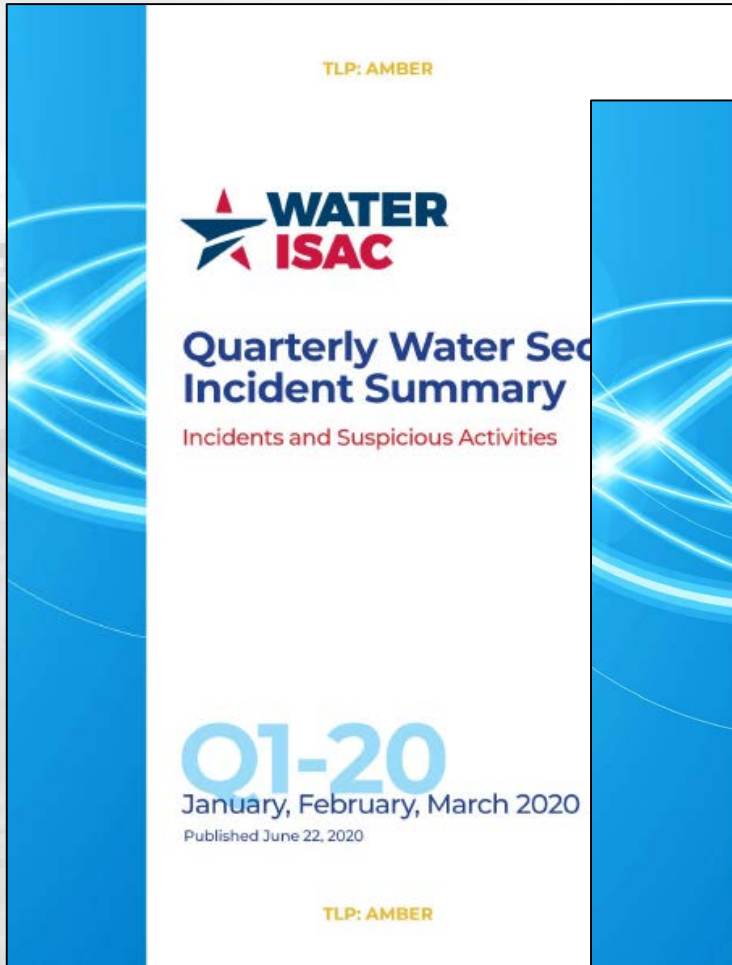
Increasing Threats and Vulnerabilities

The alert notes that adversaries have increased their capabilities and activities while vulnerabilities in critical infrastructure have grown. Some of these vulnerabilities are due to the continued use of unsecured, legacy OT assets and the increasing prevalence of internet-accessible devices, which are easy for threat actors to find.

Recommended Measures to Take Immediately

The alert describes the measures it recommends all critical infrastructure organizations take, which it says are critical for immediate implementation

Threat and Incident Reports



Guides



15 Cybersecurity Fundamentals for Water and Wastewater Utilities

Best Practices to Reduce Exploitable
Weaknesses and Attacks


2019
waterisac.org/fundamentals

1. Perform Asset Inventories
2. Assess Risks
3. Minimize Control System Exposure
4. Enforce User Access Controls
5. Safeguard from Unauthorized Physical Access
6. Install Independent Cyber-Physical Safety Systems
7. Embrace Vulnerability Management
8. Create a Cybersecurity Culture
9. Develop and Enforce Cybersecurity Policies and Procedures
10. Implement Threat Detection and Monitoring
11. Plan for Incidents, Emergencies, and Disasters
12. Tackle Insider Threats
13. Secure the Supply Chain
14. Address All Smart Devices (IoT, IIoT, Mobile, etc.)
15. Participate in Information Sharing and Collaboration Communities


<https://www.waterisac.org/fundamentals>

Webcasts and Training

Monthly Cyber Threat Web Briefings



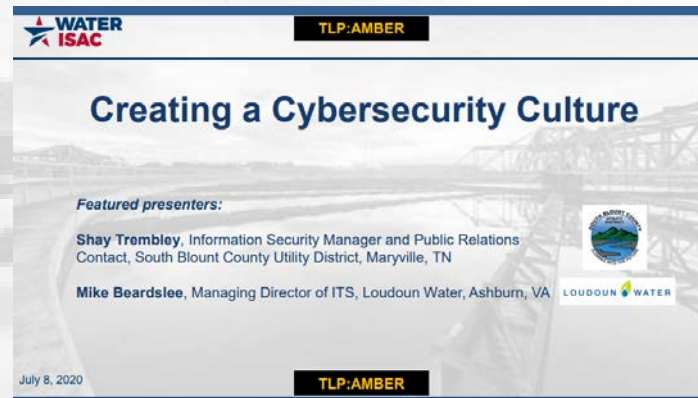
WATER ISAC
SUPERCHARGE YOUR SECURITY



**Water Information Sharing
and Analysis Center**

**Water Sector Monthly Cyber Threat Web Briefing
September 23, 2020**

Recent Webinars



WATER ISAC TLP:AMBER


Creating a Cybersecurity Culture

Featured presenters:

Shay Trembley, Information Security Manager and Public Relations Contact, South Blount County Utility District, Maryville, TN

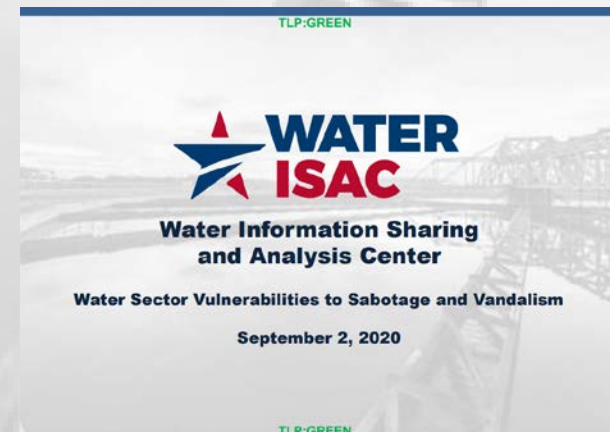
Mike Beardslee, Managing Director of ITS, Loudoun Water, Ashburn, VA

July 8, 2020 TLP:AMBER




UNITED STATES OF AMERICA
**CYBERSPACE
SOLARIUM
COMMISSION**

Water ISAC
July 1, 2020



TLP:GREEN



**Water Information Sharing
and Analysis Center**

Water Sector Vulnerabilities to Sabotage and Vandalism

September 2, 2020

TLP:GREEN

Membership

- Water and wastewater utilities
 - C-Suite
 - IT and OT
 - Security and emergency management
 - Water quality, planning, and communications
- Consulting and engineering firms
- State/provincial and federal agencies
- Law enforcement, fusion center, and homeland security personnel

Groups and Events

- Water Sector Coordinating Council
- EPA Water Security Division
- DHS Working Groups
- Conferences and Regional Meetings

Cyber Incidents and Threat Activity Against Water Utilities

Member reported – ICS/OT

- *Constant scanning*
- Malware on cellular modem at sewer lift station; device subsequently used in a DDoS attack
- CCTV feed to foreign country discovered after firewall upgrade
- Unauthorized contractor laptop connected to UV treatment system for updates
- Ransomware

Cyber Incidents and Threat Activity Against Water Utilities

Member reported – Business/Enterprise Systems

- Ransomware
- Denial of Service
- Phishing
 - Emotet
 - Impersonation-based phishing (EAC, BEC, VEC)
 - payroll diversion, gift card, invoice fraud, credential harvesting
- Insider Threats
- Website defacements
- Website compromises (injection)
- Sextortion
- USBs
- Click2Gov and other payment portal compromises
- Malware

Cyber Incidents and Threat Activity Against Water Utilities

Other sources (OSINT/trusted partners)

- 2018 – Cryptocurrency miner on OT network
- 2018/2019 – Municipality ransomware
- 2019 – Valdosta sewage spill (insider threat)
- 2020 – Israeli Water Infrastructure (3)
- 2020 – Ransomware incident at concrete firm (EFCO)

Cyber Threat Concerns to Water and Wastewater Systems

Other cyber threat/risk concerns to the w/ww sector

- ICS process aware ransomware (EKANS)
- Threats to safety (TRISIS/TRITON)
- Insider threats
- Commodity threats (phishing, malware, ransomware)
- Lack of asset management
- Deficient in vulnerability management
- Lack of incident response plans

Cybersecurity Resources and Tools for Water Utilities

EPA

- Cybersecurity Incident Action Checklist
- VSAT

WaterISAC

- 15 Cybersecurity Fundamentals for Water and Wastewater Utilities

AWWA

- Cybersecurity Guidance & Tool
- Cybersecurity Risk & Responsibility in the Water Sector

CISA

- CSET and other services



Disinformation and Water Security

Mikko McFeely

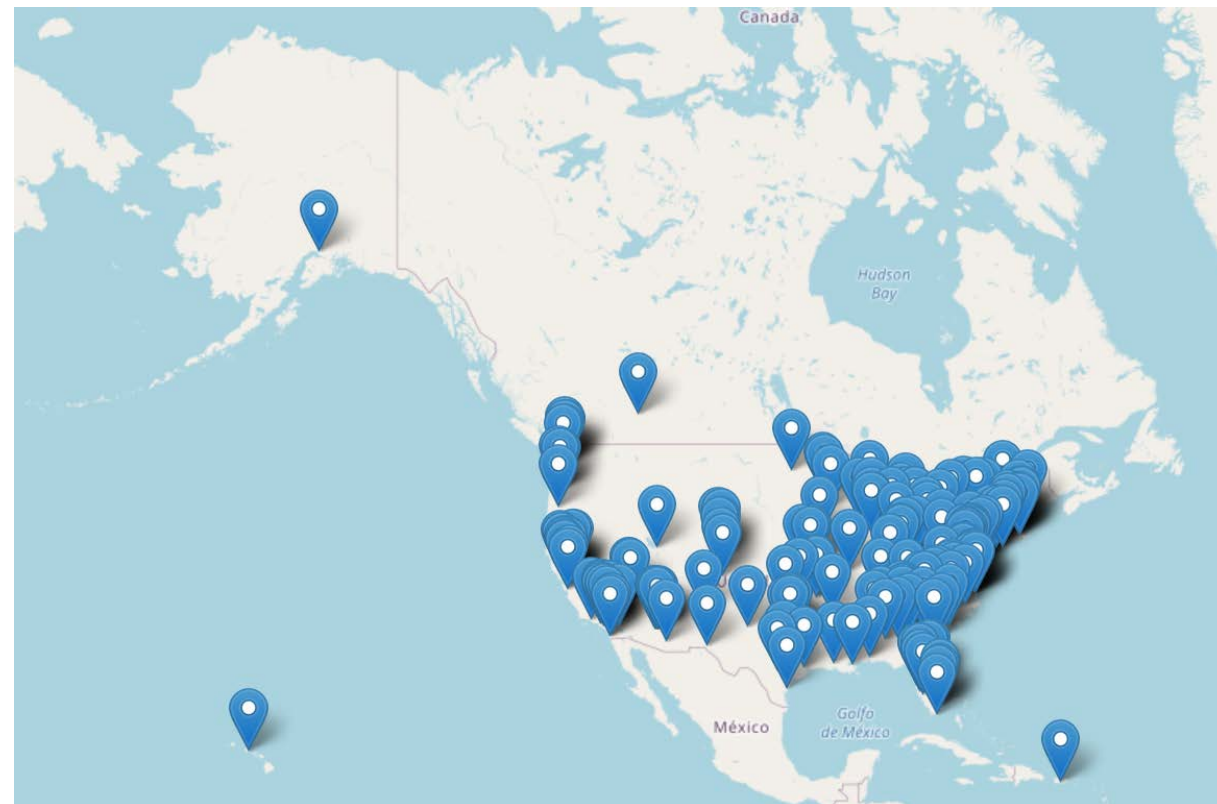
Manager of Resilience and Sustainability Affairs

Association of Metropolitan Water Agencies



About AMWA

- Represents the nation's largest public drinking water utilities
- A forum for utility general managers and senior executives
- Focuses on regulatory, legislative, utility management, and security issues





AMWA Security Products

- Sustainability and Security Report
- Webinars
- Joint products
 - Business Continuity Planning for a Pandemic: A Reference Guide
 - Countering Drinking Water Disinformation: Protecting Public Health from Malicious Messaging



Disinformation

- Inaccurate information spread with malicious intent
- Intent matters
 - Disinformation is deliberately inaccurate
 - Misinformation is incorrect



Why it matters

- Disinformation campaigns can undermine the public's trust in its drinking water
- False reports may negatively affect the operations of critical partners
- Campaigns can capitalize on an existing incident to frustrate an existing response effort



Countering disinformation

- Proactive communication
- Collaboration with response partners
- Exercises
 - Engage and include public information staff

Countering Drinking Water Disinformation
Protecting public health from malicious messaging



Reporting suspicious activity

- If you suspect you are being targeted by a disinformation campaign, contact your local FBI field office
- Report disinformation campaigns to WaterISAC

Thank You!

Nelson Mix

*Office of Water, Water Security Division
USEPA*

Mix.Nelson@epa.gov

Chuck Egli

*Lead Analyst
WaterISAC*

egli@waterisac.org

Mikko McFeely

*Manager of Resilience and Sustainability Affairs
AMWA*

mcfely@amwa.net

Jennifer Lyn Walker

*Cybersecurity Risk Analyst
WaterISAC*

walker@waterisac.org



Post Webinar Actions

Download EPA WSD Resources Document.

Complete webinar evaluation.

Join the EPA Water Security Division mailing list to receive updates and other information.

Join Us For Our Next Webinar!

Utility Webinar: Hazard Mitigation Funding

November 2020

