H2OSecCon
OCTOBER 19 - 20 ● VIRTUAL
Powered by WATER ISAC

Schedule as of October 12
Sessions and speakers are subject to change.

DAY ONE
THURSDAY, OCTOBER 19

10:00 AM - 10:45 AM **Opening General Session** **Main Stage**

- Speakers:
  - Jen Easterly, Director of Cybersecurity and Infrastructure Security Agency (CISA)
  - John Sullivan, Water Information Sharing and Analysis Center
  - Tom Dobbins, Water Information Sharing and Analysis Center

10:45 AM - 11:45 AM **Session I** **Cybersecurity Track**

Show Me the Money! Obtaining Support and Funding for Cyber Resilience Solutions

Water and wastewater treatment facilities and agencies have the unique challenge of being subject to the political and budgeting constraints of most public agencies while having to protect life- and mission-critical assets from the most sophisticated and persistent nation-state sponsored threat actors. This panel discussion will examine how other agencies have been able to align government and internal politics, secure budgeting, navigate the selection process, and select and deploy solutions that provide coverage and protection for the IT and OT environments.

- Moderator: John Minasyan, LMNTRIX
- Panelists:
  - Robert Grantham, Rancho Water
  - Jabob Margolis, Metropolitan Water District of Southern California
  - Frank Ury, Santa Margarita Water District

Session I **Physical Security Track**

Physical Security Threats to Water and Wastewater Utilities

Join a panel of experts as they break down the increasingly complex physical threat environment water and wastewater utilities face. The panelists will provide an overview of the threats posed by different malicious actors, from domestic violent extremists and foreign terrorist organizations to common criminals and insiders. They will also discuss these actors' tactics, which have been demonstrated in real-world incidents and discussed in extremist publications and online forums.

- Moderator: Andy Jabbour, Gate 15
- Panelists:
  - Alec Davison, Water Information Sharing and Analysis Center
  - John Martin, EPA's Office of Homeland Security
  - Charles Porter, DHS Office of Intelligence and Analysis

11:45 AM - 12:15 PM **Break**

12:15 PM - 1:45 PM **Session II** **Cybersecurity Track**

How Engineering Can Limit Physical Consequences of a Cyber Incident

If you can imagine a worst-case cyber threat scenario that could cause physical damage to Industrial Control System (ICS) equipment, so will the bad guys. By installing solutions to limit physical damage that could occur due to a cyber attack (or even an unintentional cyber incident/device failure), asset owners can significantly reduce the impact posed by dangerous conditions that could result in high-consequence events such as excessive levels of pressure or chemical additions. This panel session will discuss how physical engineering solutions can protect against the impact of cyber incidents, highlight multiple implementation case studies, and share examples that any water and wastewater utility can implement. The discussion will emphasize Idaho National Laboratory's Consequence-driven Cyber-informed Engineering (CCE) methodology.

- Moderator: Victor Atkins, 1898 & Co.
- Panelists:
  - Colin Dunn, Fend Incorporated
  - Sarah Freeman, MITRE's Cyber Infrastructure Protection Innovation Center
  - Jodi Jensen, Secure SCADA Solutions, LLC
  - Ian Rohrbacher, City of Rochester, New Hampshire

Session II **Physical Security Track**

Critical Infrastructure Security Vulnerabilities

During a series of three presentations, learn about how threat actors have and could exploit security vulnerabilities in critical infrastructure to conduct attacks. The presentations include an analysis of recent attacks against electric substations, including those that occurred late last year in North Carolina; a discussion of how explosives could be used to attack infrastructure, referencing tactics shared in the recently released "How to Blow Up a Pipeline" film; and an overview of vulnerabilities in the water and wastewater sector as identified by the Cybersecurity and Infrastructure Agency (CISA), through its physical security assessments of utilities.

- Speakers
  - Benjamin Gibson, Electricity Information Sharing and Analysis Center
  - Jaysen Goodwin, CISA's Infrastructure Security Division

- Felix Pomponi, CISA's Infrastructure Security Division
- Andrew Wenzel, Texas A&M Engineering Extension Services

1:45 PM – 2:00 PM **Break**

2:00 PM – 3:00 PM **SPECIAL WEBINAR FOR ALL ATTENDEES**

Securing the Flow - Advancing Public Water Systems Cybersecurity and Resilience

Hosted with CISA, EPA, and MS-ISAC

The Environmental Protection Agency (EPA), Cybersecurity and Infrastructure Security Agency (CISA), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Water Information Sharing & Analysis Center (WaterISAC) jointly host a new series designed to empower and enhance the cybersecurity and resilience of public sector water infrastructure. This educational session is specifically designed to provide actionable guidance and best practices for professionals who manage state, municipal, tribal, and territorial water systems.

3:00 PM - 3:15 PM **Break**

3:15 PM – 4:00 PM **Session III** **Cybersecurity Track**

What if the Next Shiny Thing Was Free?

Bolstering cyber resilience isn't always about buying the next shiny thing or spending millions of dollars on a product or service. For years, government and industry have been asked to step up or pay it forward and offer free resources to help ICS/OT entities improve cybersecurity. This session includes an overview from three organizations who have stepped up in a BIG way with practical and actionable resources to help water and wastewater utilities bolster cyber resilience and they don't cost you a penny!

- Speakers:
  - Dawn Cappelli, Dragos Operational Technology – Cyber Emergency Readiness Team
  - Karen Evans, Cyber Readiness Institute
  - Adam Hahn, MITRE

Session III **Physical Security Track**

Understanding Hostile Events to Prevent and Mitigate Incidents

Learn how to prevent and mitigate "hostile events" during this presentation, which will provide an overview of incidents like active shooters, workplace violence and workplace attacks, lone actor and low-tech terrorism, complex coordinated terrorist attacks, fire as a weapon, and weapons of mass destruction attacks. An important part of prevention and mitigation is also understanding the "Hostile Events Attack Cycle," or "HEAC," which refers to

the numerous stages perpetrators typically go through prior to, during, and following an attack. Utilities can use all this knowledge to improve their security, ideally preventing attacks from occurring but at the very least minimizing impacts.

- Speaker: David Pounder, Gate 15

4:00 PM – 5:00 PM **Session IV** **Cybersecurity Track**

Unlocking Secure SCADA Remote Access: Navigating the Hidden Risks

Discover the hidden dangers of remote connectivity in SCADA systems. Real-world experiences reveal that organizations often unwittingly expose their systems to the internet and other untrusted networks. Even when they acknowledge the need for remote access, many struggle to establish a minimum level of security. Join us in this talk to learn how to identify devices with internet or remote network communication capabilities and explore the essential architectures and features that fortify SCADA remote access.

- Speaker: Gus Serino, I&C Secure, Inc.

Session IV **Physical Security Track**

How to Develop a Comprehensive Resilience Program at Your Utility

This presentation will focus on the development of a comprehensive resilience program for water utilities. It will walk through the implementation of available standards and guidelines within the water space to meet legislative, organizational, and general industry best practices related to risk assessment, resilience planning, and emergency management. It will also include a case study outlining the success of one water utility in building a resilience assessment and emergency planning program that considers physical, electronic, cyber, and natural hazard threats to their utility. The goal of the presentation is to provide a roadmap for increasing the overall resilience of our nation's water infrastructure.

- Speakers:
  - Shawn Corrigan, Carollo Engineers
  - George Whitten, Carollo Engineers

DAY TWO
FRIDAY, OCTOBER 20

10:00 AM - 10:30 AM **Opening General Session** **Main Stage**

- Speaker: Kevin Morley, American Water Works Association

10:30 AM - 12:00 PM **Session V** **Cybersecurity Track**

Fear Free! Using Regulation as a Friend, Not a Foe

Take the EPA and AWIA inspection requirements to create a roadmap for cyber hygiene success. Don't fear the sanitary inspectors, use their guidance to your advantage and work towards safer environments. Use compliance to

build effective programs that protect and inform, without fear mongering. Remove the “this won’t happen here” and replace it with “we are protecting our systems in the best ways we can.”

- Moderator: Mea Clift, Woodard & Curan
- Speakers:
  - Yvette DePeizea, MassDEP Drinking Water Program
  - Bob Scott, NH Department of Environmental Services
  - Donald Wells, Luminary Automation, Cybersecurity & Engineering

Session V **Physical Security Track**

New Strategies in Resilience Planning & Drones Threat Awareness, Prevention, and Mitigation

This session will be comprised of two presentations that explore new strategies for water and wastewater utilities to improve their resilience as well as that of their partners. The first presentation will discuss the proactive application of National Incident Management System (NIMS) and its Incident Command System (ICS) principles for all-hazards contingency planning of capital improvement construction projects. The second presentation will report on the findings from a Water Research Foundation (WRF) project whose purpose is to provide case studies of infrastructure interdependencies with the water and wastewater sector and demonstrate how utilities increased their organizational resilience and sustainability.

Drones, or Unmanned Aerial Systems (UASs), continue to represent a threat to critical infrastructure, as demonstrated by real world incidents involving water and wastewater utilities as well as against other sectors. To help safeguard these critical assets and ensure their security, this session will examine the multiple threats posed by drones and understand the potential countermeasures for confronting them.

- Speakers:
  - Eric Hatcher, AECOM
  - Travis Moran, SERC Reliability Corporation

Noon - 12:30 PM **Break**

12:30 PM - 1:15 PM **Session VI** **Cybersecurity Track**

Increase PLC Integrity with the Top 20 Secure PLC Coding Practices

Programmable Logic Controllers (PLCs) are often (and aptly) described as insecure-by-design, but they don’t have to stay that way! This session will introduce attendees to the first of its kind guidance resource to help secure those inherently insecure-by-design devices. The Top 20 Secure PLC Coding Practices were written by engineers for engineers and technicians that program and maintain PLCs. During this session attendees will learn how native functionality can be leveraged to securely program PLCs with little to no additional software tools or hardware. Most importantly you’ll walk away with a

few quick win practices to implement now to begin increasing PLC integrity, monitoring, hardening, and resilience at your utility.

- Speaker: Vivek Ponnada, Nozomi Networks

Session VI **Physical Security Track**

Preparing Your Employees and Communities for Emergencies

For any organization to be prepared for an emergency, its employees also must be individually prepared and able to assist with the response. Additionally, there's much organizations, water and wastewater utilities included, can do to help prepare their communities for emergencies, especially when the critical services they provide may be impacted. This session is intended to help water and wastewater utilities think through important considerations and resources in these regards, covering employee capacity building, hazard based protective actions, citizen responder programming, youth preparedness, and the Homeland Security Grant Program.

- Speaker: Aaron Levy, FEMA's Individual and Community Preparedness Division

1:15 PM - 2:00 PM **Session VII** **Cybersecurity Track**

Human Crown Jewels: How to Protect High Value Targets and Prevent Compromise

Nearly every major attack relies on social engineering somewhere in the attack chain. Rather than rely on detection and response capabilities alone, defenders can "defend forward" and take proactive measures to prevent attacks before they happen by protecting high-value (human!) targets. This is not another talk about awareness training, but rather about how to protect the "human attack surface" of your organization.

- Speaker: Matt Polak, Picnic

Session VII **Physical Security Track**

Increasing Resilience of the Water and Wastewater Sector to Supply Chain Disruptions

For this session, a panel of experts will discuss the potential for supply chain disruptions in the sector, impacting critical materials like chemicals but also equipment and parts. They will draw from the experiences of recent supply chain issues and examine various strategies and measures for utilities to improve their resilience to these events.

- Moderator: Chuck Egli, Water Information Sharing and Analysis Center
- Speakers:
  - Steve Allgeier, EPA's Office of Ground Water and Drinking Water, Water Infrastructure and Cyber Resilience Division
  - Hugh-Berk Sinclair, Arcardis
  - Matt Umberg, EPA's Office of Ground Water and Drinking Water, Water Infrastructure and Cyber Resilience Division

2:00 PM - 2:30 PM **Closing General Session** **Main Stage**

- Nitin Natarajan, Deputy Director of Cybersecurity and Infrastructure Security Agency

2:30 PM - 2:45 PM **Break**

2:45 PM – 5:00 PM

TTX* **Cybersecurity Track**

Cyber Security Tabletop Exercise (TTX) – Priority is in the Eye of the Asset Owner

If everything is a priority, nothing is a priority. There are multitude types of cyber attacks that can cripple an OT system resulting in cyber-physical impacts to a utility, the public, and even community response resources. There's no doubt that ransomware has had significant impact on numerous critical infrastructure organizations. But is ransomware the biggest threat to YOUR utility, operations, constituents, or community at large?

This session is more than the usual tabletop exercise that dissects response to an arbitrary (albeit important), headline making threat. This exercise will:

- Help asset owners choose and prioritize the most impactful OT scenario to prepare for and execute a TTX.
- Provide ways to assess the impacts of a cyber incident beyond the technical ramifications.
- Demonstrate a method for determining a standardized priority score to understand how various OT scenarios might impact different targets in different ways.

Facilitator: Danielle Jablanski, Nozomi Networks

TTX* **Physical Security Track**

Physical Security Tabletop Exercise (TTX) - Preparing for and Responding to Hostile Events

The focus of this TTX will be preparing for hostile events, expanding on the scenario utilized last year and including new threat vectors and attack targets. During the TTX, players will participate in a discussion-based scenario facilitated by WaterISAC staff. Attendees will have the opportunity to voice mitigation strategies or recommend best practices for preventing or mitigating threats. Overall, the TTX will highlight skills to recognize and better prepare for and react to a hostile event.

Facilitators:

- Alec Davison, Water Information Sharing and Analysis Center
- Chuck Egli, Water Information Sharing and Analysis Center

**TTX sessions require an additional registration and have limited access.*