# $H_2O$SecCon

VIRTUAL 2024

Powered by WATER ISAC

*Schedule as of April 24*
*Sessions and speakers are subject to change.*

## THURSDAY, MAY 23

**11:00 AM - 11:30 AM**

### OPENING

*Combined Track*

*Speaker:* **Brian Harrell,** Vice President & Chief Security Officer of Avangrid

**11:30 AM - 12:30 PM**

### SESSION I

*Cybersecurity Track*

***Lessons and Insights Securing Critical Infrastructure: A Combined Century of Hands-on Experience***

What do you get with four seasoned cybersecurity professionals? Actionable advice and prudent counsel from over a century of combined experience in tackling the complexities of cybersecurity within critical infrastructure.

This panel session brings insights, lessons learned, and perspectives from four accomplished professionals in the field of cybersecurity from varying disciplines - two who grew into cybersecurity from career roots in operational technology (OT) and two who began their careers as IT professionals and leaders. Panelists will share successes, failures, do-overs, and even times they needed to stand their ground in the face of impractical directives that could've threatened security. There will be technical insights, pro-tips, and knowledge on crucial soft skills that can make or break critical cyber strategy - there may even be respectful debates and lighthearted differences of opinion.

Attendees will glean technical and cultural guidance to readily apply at their utility to make the cybersecurity journey more smooth, effective, efficient, and successful - and hopefully less of a challenge.

*Moderator:* **Gus Serino,** I&C Secure

*Panelists:* **Geoffry Brown,** Alameda County Water District
**Tung Nguyen,** Denver Water
**Don Wells,** Luminary A.C.E.

### SESSION I

*Physical Security Track*

***Extremists, Terrorists, and Common Criminals – What Utilities Need to Know about Today's Physical Security Threats to Critical Infrastructure***

Join a panel of experts from the federal government (including the FBI and DHS), academia, and WaterISAC 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:* **Chuck Egli,** *WaterISAC*

*Panelists:* **Seamus Hughes,** *University of Nebraska-Omaha*
*Representatives from DHS and the FBI*

**12:30 PM - 1:00 PM** **BREAK**

**1:00 PM - 1:50 PM**

## SESSION II

*Cybersecurity Track*

### *Engineering-Grade OT Security for Water Systems*

The Cyber-Informed Engineering (CIE) methodology points out that critical infrastructures demand engineering-grade protections from cyber attacks, not only conventional cybersecurity protections. Engineering-grade protections are deterministic, with mathematically modellable failure rates - these techniques are in a real sense, “unhackable.”

This session reviews threats, as well as water and wastewater systems and other infrastructures shut down recently by cyber attacks. We look at physical processes in water systems and draw conclusions about worst-case consequences (high-impact rather than high-frequency attacks). We then dig into the emerging body of knowledge that is CIE, including parts of safety, protection, and network engineering, and look at which protections are most applicable to which kinds and scales of water systems. Finally, we explore the emerging field of network engineering techniques for preventing even nation-state-grade cyber attacks from pivoting into OT/control systems.

*Speaker:* **Andrew Ginter,** *Waterfall Security*

## SESSION II

*Physical Security Track*

### *Online Threats of Violence – Observed Crossover between Electricity and Water and Wastewater Sectors*

This session will feature a joint presentation by Electricity-ISAC (E-ISAC) and WaterISAC analysts. It will begin with a discussion of the E-ISAC’s online threat monitoring framework, including collection practices and methods, online threat categorization and assessment criteria, and a high-level analytical summary of the types of online threats that have been observed since 2023. In this presentation, additional insight will be discussed regarding observed online threats referencing violence towards both the water and wastewater and electricity sectors, including a discussion of notable extremist publications in addition to singular instances of online threatening discourse. The presenters will also cover how online publications and discourse on tactical recommendations have manifested in real world incidents.

*Speakers:* **Alec Davison,** *WaterISAC*
*Representatives from E-ISAC*

**1:50 PM – 2:00 PM** **BREAK**

**2:00 PM – 2:50 PM**

## SESSION III

*Cybersecurity Track*

### *Preventing the Terminator: AI-Resistant OT Cybersecurity Protection*

Generative AI is changing Water and Wastewater OT Network Managers’ threat landscape, as threat vectors like phishing and reconnaissance are turbo-charged by tools like ChatGPT, WormGPT, and FraudGPT. Existing IT-oriented solutions cannot prevent these attacks today and are powerless against the enhancements. How can OT network managers prevent these threats from infiltrating their OT network? This session will explore breaking the cyber kill chain that relies on these initial threat vectors.

*Speakers:* **Joe Baxter,** *BlastWave*
**Cam Cullen**, *BlastWave*
**Vince Zappula,** *BlastWave*
**Scott Christensen,** *GrayMatter*

**2:00 PM – 2:50 PM**

**SESSION III** *Physical Security Track*

***High-Impact, Low/No-Cost Solutions to Build and Improve Your Utility's Physical Security***

Security solutions to address threats and vulnerabilities at water and wastewater utilities: utilities of all sizes face an increasingly complex physical threat landscape as they work to provide critical services for their communities. Join us for an in-depth discussion with a fellow water and wastewater utility security manager and a CISA protective security advisor (PSA) as they discuss low/no-cost solutions and opportunities for organizations to implement now to increase their security and resilience. Topics covered will include perimeter security design, security staffing, the PSA program, understanding grants, and more.

*Speakers:* **Dave Cole,** *Metropolitan Water District of Southern California*
**Scott Mitchem,** *CISA Region 9*

**2:50 PM - 3:00 PM**

**BREAK**

**3:00 PM – 3:50 PM**

**SESSION IV** *Cybersecurity Track*

***System Hardening: Locking the Doors and Closing the Drapes***

Every major cybersecurity guideline, including AWWA, includes hardening as a recommended component. The sheer number of settings per component and components per facility often dissuades companies from doing more than just scratching the surface of this highly effective method of reducing the attack surface. This presentation will discuss the different types of system hardening and examine the pros and cons of different implementation and auditing methods – manual, script-based, and fully automated – in IT, OT, and DMZ environments. Additionally, the presentation will examine the two major system hardening standards, CIS and STIG, and discuss building a custom standard derived from one of these standards.

*Speaker:* **Joe Cody,** *EIS*

**SESSION IV** *Physical Security Track*

***Preparing for Water Scarcity: Water Sector Operational Resilience to Severe Drought***

During this session, Dr. Michael Cohen of MITRE will provide a briefing that documents a case study performed for the Lower Colorado River area of Texas concerning how to make a region of the county resilient to long-term severe drought. The case study examines water supply and demand reduction/efficiency options and demonstrates how to evaluate the costs and benefits of the individual options, rank order them, as well as how to estimate the benefit to the regional economy from avoiding a severe long-lasting drought. With drought and other significant water scarcity issues in recent times, utilities shouldn't miss out on this opportunity to learn how they can build resilience for these challenges.

*Speaker:* **Michael Cohen**, *MITRE*

**3:50 PM - 4:00 PM**

**BREAK**

**4:00 PM – 4:50 PM**

## SESSION V

*Cybersecurity Track*

### *Stories from the Field: Cybersecurity Incidents and Improvements*

This session will highlight the case studies published by WaterISAC and US EPA to demonstrate how cyber incidents can occur and the steps other utilities have taken to protect themselves against these threats. WaterISAC will provide information and insight on their case studies highlighting real-world examples of cybersecurity incidents at water and wastewater utilities. This presentation will go through all phases of each incident including a description, impact, response, and lessons learned. US EPA's Water Infrastructure and Cyber Resilience Division will present case studies which highlight the cybersecurity programs of utilities that decided to act and improve their cybersecurity posture. This presentation will demonstrate each utility's cybersecurity improvements and lessons learned throughout the process of improving their cybersecurity.

*Speakers:* **Cole Dutton,** *EPA*
**Andrew Hildick-Smith,** *WaterISAC*

## SESSION V

*Physical Security Track*

### *Balancing the Desire for Transparent Communications with Your Stakeholders While Maintaining the Need for Secrecy*

Presenters from the Northeast Ohio Regional Sewer District (NEORSD) will share how their utility balances its core philosophy of transparency while also protecting sensitive information. Although much of its work is underground, NEORSD wants to ensure stakeholders know who it is, what it does, and why its work is important. To that end, it has a formal public engagement statement that assures communication will be timely, truthful, thoughtful, and two-way. However, the communicators' need for full transparency oftentimes conflicts with emergency managers' need for secrecy. So what happens when the organization's communications team wants to promote infrastructure investment? Host a large-scale public event? Tour facilities? Share the process behind the work of NEORSD's more than 750 employees working 24/7/365 for clean water? When it comes down to it, it's simple: collaboration, shared common operating procedures, and trust.

*Speakers:* **John Corn,** *NEORSD*
**Jenn Elting,** *NEORSD*

**4:50 PM - 5:00 PM**

## INDIVIDUAL TRACK CLOSINGS

*Both Tracks*