DAY ONE | Physical Security & Resilience

November 15, 2022 - All times are in EST

12:30 PM - 1:15 PM
Opening Remarks & Main Stage Speaker

- Seamus Hughes | *Deputy Director*, George Washington University, Program on Extremism

1:15 PM - 2:15 PM
SESSION I: **Physical Security Threats to Water and Wastewater Systems**
Water utilities continue to face an increasingly complex physical threat environment. Join a panel of experts as they provide an overview of the threats posed by different malicious actors, from domestic violent extremists and foreign terrorist organizations to common criminals and insiders.

- Moderator
  - Andy Jabbour | *Co-founder and Managing Director*, Gate 15

- Panelists
  - Angie Gad | *Director of Analysis,* Alethea Group
  - Alec Davison | *All-Hazards Risk Analyst*, WaterISAC
  - Bridget Johnson | *Managing Editor*, Homeland Security Today
  - Luke Citro | *Intelligence Analyst*, Federal Bureau of Investigation

2:15 PM - 2:30 PM
Break

2:30 PM - 3:30 PM
SESSION II: **Reducing Physical Security Risks: Solutions for Utilities**
All utilities face similar threats while providing a critical service to their communities. Join industry emergency management and security practitioners as they detail solutions that can be implemented to face those challenges.

- Moderator
  - Steve Bieber | *Water Resources Program Director*, Metropolitan Washington Council of Governments, and *President*, InfraGard National Capital Region

- Panelists
  - Vicki White | *Director of Commercial Water Services*, Herndon Solution Group
  - William McNamara | *Protective Security Advisor - National Capital Region,* Cybersecurity and Infrastructure Security Agency (CISA)
  - David Paulos | *Area Vice President,* GardaWorld

3:30 PM - 4:30 PM
SESSION III: **Lessons Learned and Best Practices Responding to Natural Disasters and Climate Change**
Every utility has had to adapt to evolving situations and learn from past events. Listen to water sector experts as they share natural disaster preparedness and response insights and discuss climate change impacts and adaptation.

- Moderator
  - Chuck Egli | *Director of Preparedness and Response*, WaterISAC

- Panelists
  - Stephen MacCarthy | *Manager of Corporate Security*, Water Corporation, Australia
  - Eric Hatcher | *Senior Emergency Preparedness Specialist*, AECOM
  - Stephanie Lavey | *Sustainability Coordinator*, Alexandria Renew

4:30 PM
Closing Remarks

DAY TWO | Physical Security & Resilience
November 16, 2022

12:30 - 1:00 PM
Welcome Remarks & Main Stage Speakers

- Rep. John Katko (R-NY) | Ranking Member, House Homeland Security Committee
- Nushat Thomas | *Cybersecurity Branch Chief*, US Environmental Protection Agency (EPA)

1:00 PM - 1:45 PM
SESSION IV: **Back to the Basics: A to Z on Cybersecurity**
Best practices and advice on cybersecurity for utilities and their employees. Understanding and how to use the resources provided by agencies, associations, and industry partners.

- Roger Caslow | *Chief Information Security Officer*, HRSD and Manager on WaterISAC Board of Managers

1:45 PM - 2:30 PM
SESSION V: **Cybersecurity Financial Risks and Insurance – You Can Offset Some Risks, But Not All**
From salaries and equipment replacement, to ransom demands, losses due to downtime, and much more, restoring systems and operations after a cyber attack can be expensive. While cyber insurance can help, it's important to understand the exclusions and what your policy won't help you recover.

- Moderator
  - Andrew Hildick-Smith | *OT Security Lead*, WaterISAC

- Speakers
  - Bob Schwarm | *IT Director,* The Metropolitan District Commission
  - Mike Beardslee | *Managing Director of IT Services,* Loudoun Water
  - John Doernberg | *National Director of Cyber Practice,* Gallagher Brokers

2:30 PM - 2:45 PM
Break

2:45 PM - 3:30 PM
SESSION VI: **Cybersecurity Culture and Leadership: Observations from the Field**
To have a strong cybersecurity program, utilities need a pervasive cyber culture and an engaged leader. Fortunately, leadership in cybersecurity can take many forms and be effective.

- Moderator
  - Andrew Hildick-Smith | *OT Security Lead*, WaterISAC

- Panelists
  - Peter Hunt | *Chief Information Officer*, Boston Water and Sewer Commission
  - Bryon Black | *Information Technology Manager*, South Coast Water District, Calif.
  - Bill Fitzgerald | *Small Community Water Systems Manager*, Northeast US

3:30 PM - 3:45 PM
Break

3:45 PM - 5:30 PM
TTX on Cybersecurity* - Are You Ready for an OT-impacting Ransomware Incident?
Attendees will have the opportunity to actively participate in an afternoon tabletop exercise developed by Dragos for its new OT-CERT (Operational Technology – Cyber Emergency Readiness Team) program. The exercise is a facilitated discussion to provide water and wastewater utility OT and IT staff (operators, engineers, analysts, managers, supervisors, executives, etc.) an opportunity to practice cyber incident response processes and procedures based on an OT-impacting ransomware incident. The exercise will also help identify areas of excellence and potential opportunities for improvement. No cybersecurity expertise is necessary!

Even if you've never thought about ransomware, it's impacting organizations and utilities of all sizes. It's also impacting OT/ICS environments more and more. This exercise will give you a jump start so you are prepared in case it happens to you.

**Additional registration was required.*

DAY THREE | Pick Your Track

November 17, 2022

Day three will open with remarks from Eric Goldstein for both Track I and Track II, then you can pick your track.

- **TRACK I:** Cybersecurity - Taking it Up a Notch, Slightly More Technical
- **TRACK II:** Physical Security - Round Two and TTX

12:30 PM - 1:00 PM
Welcome & Remarks

- Eric Goldstein | *Executive Assistant Director for Cybersecurity*, Cybersecurity and Infrastructure Security Agency (CISA)

TRACK I
1:00 PM - 1:45 PM
SESSION VII - TRACK I: Baseline Cross-Sector Cybersecurity Performance Goals
CISA in collaboration with NIST and other organizations and individual subject matter experts, has created a document for voluntary use by critical infrastructure sectors that identify a prioritized list of recognized risk reduction measures. Known as the Baseline Performance Goals (BPGs), they are consistent with the NIST Cybersecurity Framework.

- Daniel Bardenstein | *New Tech and Cyber Strategy Lead*, Cybersecurity and Infrastructure Security Agency (CISA)

1:45 PM - 2:30 PM
SESSION VIII: MITRE ATT&CK® for Industrial Control Systems – Common Knowledge Base for Communicating Malicious Behaviors
The MITRE ATT&CK® Knowledge Base provides a repository of common terminology for network defenders to communicate about real-world attacks. ATT&CK® for Industrial Control Systems builds on ATT&CK® by describing specific post-compromise actions and behaviors unique to attacks on ICS environments.

- Otis Alexander | *Principal Cyber Security Engineer*, MITRE

2:30 PM - 2:45 PM
Break

2:45 PM - 3:30 PM
SESSION IX: Secure Remote Access for ICS/OT/SCADA – When You Absolutely, Positively Can't Live Without It
While it's preferable to prohibit remote access into an OT network, that's often not the practical choice. For those times when you absolutely, positively need remote access, learn pragmatic, low-cost methods for doing it securely and about the risks when you don't.

- Gus Serino | *Principal ICS Security Analyst*, Dragos

3:30 PM - 4:15 PM
SESSION X: The Importance of ICS/OT Monitoring – Just Because We Can't See Them, Doesn't Mean They Aren't There
Presently, we have much more visibility on our IT networks, but threat actors aren't just attacking IT. In order to know who is after our OT environments, we need better visibility into them.

- Michael Toecker | *Cybersecurity Advisor*, Department of Energy (DOE)

4:15 PM
Event Closing Remarks

TRACK II
1:00 PM - 2:00 PM
SESSION VII - TRACK II: Recognizing and Responding to the Early Indicators of Hostile Events
As conference attendees will already have learned, water and wastewater utilities face physical security threats from a range of actors, including external entities like domestic violent extremists and common criminals but also insiders from within their own organizations. No matter where they come from, one thing all threat actor have in common is that they typically display early indicators suggesting they're planning to or might conduct a hostile act. For this session, a team of speakers from DHS will review the indicators and other suspicious activities to look out for and how to respond to them, including by reporting them to the appropriate authorities. Don't miss this opportunity to receive important information that can help your utility prevent and mitigate what could otherwise become a very impactful incident.

2:00 PM - 2:15 PM
Break

2:15 PM - 4:15 PM
TTX on Physical Security* - Preparing for Hostile Events
At this TTX we will be discussing and preparing for hostile events. Hostile Events include active shooter incidents, workplace violence and workplace attacks, lone actor and low-tech terrorism, complex coordinated terrorist attacks, fire as a weapon, weapons of mass destruction, and other related activities. The hostile event attack cycle incorporates the seven phases threat actors utilize when planning and conducting attacks.

During the TTX, players will participate in a discussion-based scenario that concerns hostile events occurring in the water sector. WaterISAC staff will facilitate discussion on the hostile event and players will have the opportunity to voice mitigation strategies or recommend best practices for preventing or mitigating threats. The TTX will provide attendees with the skills needed to recognize types of hostile events, to better prepare for and react to an event; identify indicators of potential violence to possibly avert a hostile event from occurring; identify the phases of a hostile event; and provide mitigation strategies to help develop a training program for your organization.

**Additional registration was required.*

4:15 PM
Event Closing Remarks