EPA Introduction to Cybersecurity Workshop and Response Exercise (Virtual)

Course Description and Presentation Descriptions

Course Description

This workshop and response exercise is directly related to managing the operation or maintenance of a wastewater system because it introduces and familiarizes the participants with the threat of a cyber attack and the consequences it could have on a water or wastewater utility. Water and wastewater utilities are heavily reliant on computers to provide service to their customers, so operators should be aware of how to identify a potential cyber attack. This training event is applicable to all water and wastewater utilities and the workshop will cover the following topics:

- Cybersecurity threat overview
- Cybersecurity drivers and resources
- Department of Homeland Security cybersecurity tools and resources
- Findings and lessons learns from Virginia water utility cybersecurity vulnerability assessments and cybersecurity technical assistance with water and wastewater utilities
- Cybersecurity program development

The response exercise is designed to foster discussion among utilities and will allow operators to discuss the information presented during the workshop presentations further. The response exercise focuses on water utility cybersecurity incident response and coordination with other internal and external entities regarding a potential attack. Participants will discuss the following topics:

1. Cybersecurity challenges.
2. Awareness of the damage that can be caused by a cyber incident on a control system.
3. Internal and external relationships essential to the success of organizational cyber incident management.

This event has several learning outcomes that participants will be able to demonstrate as a result of their attendance. As a result of the workshop they should:

- Understand the threat of cyber attacks to a water or wastewater plant
- Learn ways to manage the threat of a cyber attack
- Receive information about tools (e.g., American Water Works Association cybersecurity tool) available to help wastewater utilities
- Receive practical lessons learned from cybersecurity assessments conducted at Virginia utilities
- Identify general planning and procedural actions to enhance cybersecurity at their own utility
- Learn and share best practices from other utilities
- Realize the importance and value of conducting tabletop exercises within their utility

Overall, water and wastewater operators will come away from this training with a better understanding of the how to approach emerging cybersecurity threats and protect their utility from harm.

Threat Overview

This presentation provides a cybersecurity threat overview specific to the water sector. It covers common attack methods, SCADA vulnerabilities, history of cyber incidents in the water sector, and

consequences of attacks to utilities. This presentation sets the stage for the participants to understand why preparing for a cyber incident is so important.

Cybersecurity Drivers and Resources for the Water Sector

This presentation presents the cybersecurity drivers for and resources available to the water sector. First, the presentation provides an overview of America's Water Infrastructure Act Section 2013, which establishes requirements for community water system's risk and resilience assessments and emergency response plans to consider and incorporate cybersecurity. The second part of the presentations presents several resources available to the water sector, including EPA's Incident Action Checklist, WaterISAC's 15 Cybersecurity Fundamentals, AWWA's Cybersecurity Guidance, and Department of Homeland Security assessments and alert notifications.

Cybersecurity Best Practices: Case Study from Virginia Waterworks Assessments and Cybersecurity Technical Assistance Project

This presentation presents results and lessons learned from two different projects: a series of cybersecurity assessments conducted with Virginia water utilities, and cybersecurity technical assistance conducted with over 100 utilities. The lessons learned that are shared during this presentation will cover common vulnerabilities found a many utilities and will cover low- to no-cost solutions to becoming more cyber secure.

Cybersecurity and Infrastructure Security Agency Resources

This presentation will be provided by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) Cyber Security Advisors (CSA). They will provide information about the diverse array of cybersecurity resources for utilities, including information sharing such as alerts and notifications, training, information for industrial control systems, and assessments.

Cybersecurity Response Exercises

Attendees will participate in two response exercises to allow further discussion of information presented during the workshop presentations. In addition, attendees will consider and discuss available resources, reporting process, and emergency response protocols in response to the scenario. The tabletop exercises are facilitator-led with scenario information presented in a series of injects. Facilitators will prompt discussion with discussion questions.

Cybersecurity Incident Response

This presentation provides an overview of cyber incident response. The presentation highlights the incident response life cycle and provides information on each stage: preparation, detection and analysis, containment, eradication and recovery, and post-incident activity. The presentation also provides available resources to help utilities develop their incident response plan.

Cybersecurity Resources/Q&A

This presentation is to showcase a variety of tools and gadgets available for utilities to use to better understand their cyber risk and vulnerabilities. The presenter provides examples of the "gadgets", but in no way promotes or endorses products, product lines, or services of a manufacturer, distributor, or

service provider. The chosen example is only used to illustrate the importance of protecting access to your internet connected devices (e.g., Supervisory Control and Data Acquisition (SCADA) systems).

- Shodan – an example of an internet search engine to locate internet-connected devices by IP address. It illustrates the importance of protecting your systems from intrusion or making them inaccessible from the web.
- Radio frequency interferences and recording example – the example he uses is a kit that can be purchased online and used to "copy" a radio frequency and operate a doorbell. It illustrates the importance of protecting your systems from web intrusion.

Records Retention Statement

A copy of the training materials and course information will be retained on file by Horsley Witten Group for at minimum of five years from the date training was offered. Copies of materials to be retained include: seminar instructional/training materials, evaluation forms, and course completion certificates.