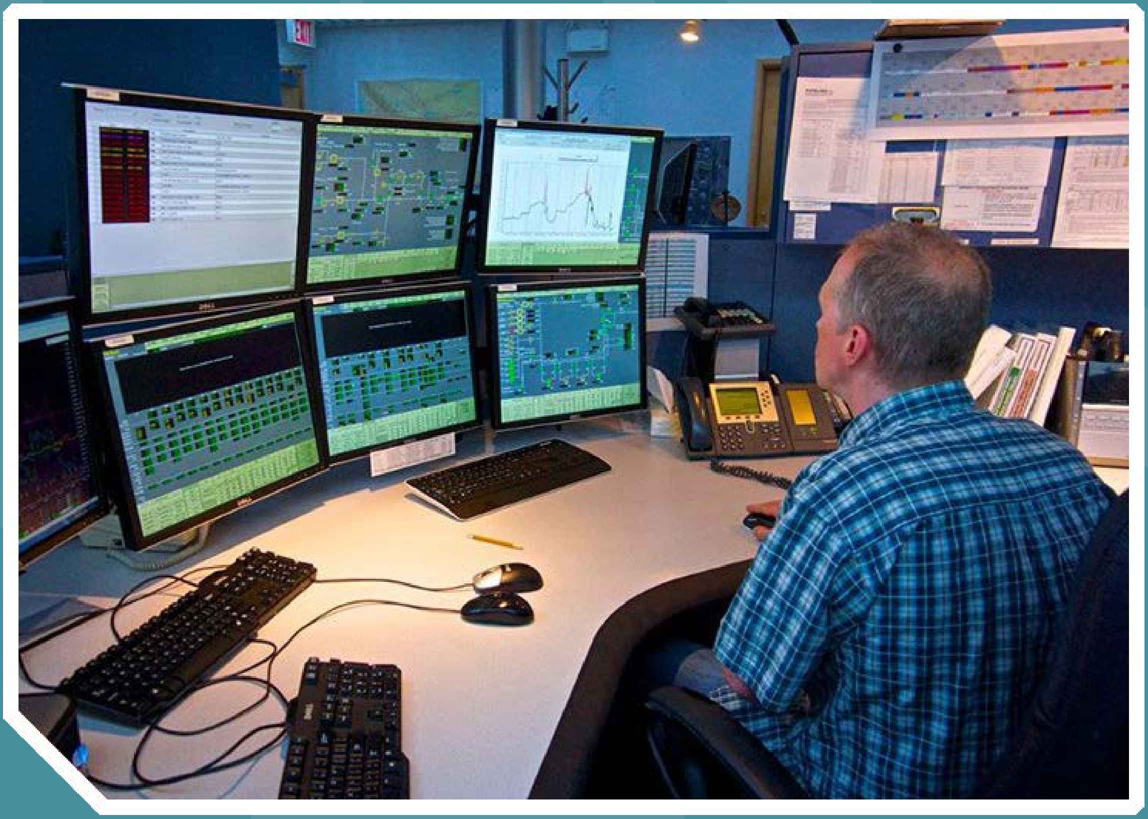
EPA
United States
Environmental Protection
Agency

EPA/600/R-17/109 | April 2017
www.epa.gov/homeland-security-research

# Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation's Water and Wastewater Systems Sector



**Office of Research and Development**
Homeland Security Research Program

This page left intentionally blank

# Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation’s Water and Wastewater Systems Sector

A Workshop Summary Report

United States Environmental Protection Agency
Cincinnati, OH 45268

April 12th, 2017

# Table of Contents

## Disclaimer

The U.S. Environmental Protection Agency (EPA), through its Office of Research and Development's National Homeland Security Research Center, funded and managed this project under contract EP-C-15-001 with Scientific Consulting Group, Inc. (Gaithersburg, MD). This report has been peer and administratively reviewed by the Agency but does not necessarily reflect the Agency's views. EPA does not endorse the purchase or sale of any commercial products or services. Mention of trade names or commercial products does not constitute endorsement or recommendation for use of a specific product.

Questions concerning this document should be addressed to:

Eric Koglin
National Homeland Security Research Center
Office of Research and Development
U.S. Environmental Protection Agency
P.O. Box 93478
Las Vegas, NV 89193
koglin.eric@epa.gov

Stephen Clark
National Homeland Security Research Center
Office of Research and Development
U.S. Environmental Protection Agency
William Jefferson Clinton Building
1200 Pennsylvania Avenue, N. W.
Mail Code: 8801R
Washington, DC 20460
clark.stephen@epa.gov

Additional technical contributors:

Dr. Hiba Ernst
National Homeland Security Research Center
Office of Research and Development
U.S. Environmental Protection Agency
26 W. Martin Luther King Dr.
Cincinnati, OH 45268

Dr. James Goodrich
National Homeland Security Research Center
Office of Research and Development
U.S. Environmental Protection Agency
26 W. Martin Luther King Dr.
Cincinnati, OH 45268

## List of Tables

# Acronyms and Abbreviations

| | |
|---|---|
| AWWA | American Water Works Association |
| BOSC | Board of Scientific Counselors |
| CIP | critical infrastructure protection |
| CIPAC | Critical Infrastructure Partnership Advisory Council |
| CSET | Cyber Security Evaluation Tool |
| DCS | distributed control system |
| DHS | U.S. Department of Homeland Security |
| DOE | U.S. Department of Energy |
| EPA | U.S. Environmental Protection Agency |
| ERO | Enterprise Reliability Organization |
| FERC | Federal Energy Regulatory Commission |
| HMI | human-machine interface |
| HSARPA | Homeland Security Advanced Research Projects Agency |
| HSRP | Homeland Security Research Program |
| ICS | industrial control system |
| ICS-CERT | Industrial Control Systems Cyber Emergency Response Team |
| IT | information technology |
| NCATS | National Cybersecurity Assessment & Technical Services |
| NCCIC | National Cyber and Communications Integration Center |
| NERC | National American Electric Reliability Corporation |
| NHSRC | National Homeland Security Research Center |
| NIST | National Institute of Standards and Technology |
| NSTC | National Science and Technology Council |
| ORD | Office of Research and Development |
| OT | operational technology |
| PCS | process control system |
| PLC | programmable logic controller |
| RTU | remote terminal unit |
| SCADA | supervisory control and data acquisition |
| SME | subject matter expert |
| UL | Underwriters Laboratory |
| UL CAP | UL Cybersecurity Assurance Program |
| WaterISAC | Water Information Sharing and Analysis Center |
| WRF | Water Research Foundation |
| WSCC CSWG | Water Sector Coordinating Council Cyber Security Working Group |

# Acknowledgements

The U.S. Environmental Protection Agency acknowledges the support provided by the organizations represented at the Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation’s Water and Wastewater Systems Sector. The report content is based on the workshop session discussions and a pre-meeting list of recommendations thoughtfully provided by the subject matter experts. Contributions to this report by all workshop participants, via expressed viewpoints during the workshop and review comments on the draft report, are duly acknowledged. The contributions of Scientific Consulting Group, Inc. (Gaithersburg, MD), Inc., under contract EP-C-15-001, are also recognized in the development of this document.

# Executive Summary

Cybersecurity has emerged as an issue of growing concern to the nation's water and wastewater utilities. Cyber-attacks on water utilities can have far reaching impacts on public health; not only in the delivery of clean, potable water to consumers but to other critical services that depend on the continuous delivery of water. In recognition of the growing need to better address cyber risk and cyber management, the U.S. Environmental Protection Agency's (EPA) National Homeland Security Research Center (NHSRC) held a Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation's Water and Wastewater Systems Sector on March 30th and 31st, 2016, at the Ronald Reagan Building in Washington, D.C. The workshop was designed to create a forum for subject matter experts (SMEs) to exchange ideas and address important cybersecurity challenges facing the water sector. The SMEs were convened to provide individual advice and recommendations that NHSRC could consider in its cybersecurity research planning efforts. At no point in the meeting were they asked for consolidated, consensus recommendations.

The workshop's **primary objective** was to engage SMEs and identify water infrastructure cybersecurity research gaps and needs. Eleven SMEs were invited to participate in the workshop and another 24 stakeholders participated as observers. The stakeholders and SMEs represented water and wastewater utilities, water trade and professional associations including consultants that have supported water utilities in cybersecurity, water associations and research organizations, and staff from a Department of Energy (DOE) National Laboratory. In addition, staff from the Department of Homeland Security (DHS) and EPA (specifically the Office of Water) also participated in the workshop.

**Key Messages and Recommendations:** The workshop participants discussed a number of important cybersecurity needs facing the water sector that included:

- Information technology/operational technology (IT/OT) system architecture
- Interdependence between cybersecurity and physical security of facilities and assets (cyber-physical)
- Communications
- Computer and process control system (PCS) software
- Regulatory and industry standards
- Water utility cybersecurity risk management
- Personnel (ability to hire qualified expertise)
- Utility size and business model
- Training and education

The main research gaps and needs identified by the SMEs for EPA's Office of Research and Development/NHSRC were:

- Cyber-physical impacts and design mitigations
- IT/OT software and monitoring design

The information and recommendations provided by the SMEs will help the Agency to develop a better understanding of the impact of cyber intrusion on water and wastewater utilities and to begin formulating a research and development approach that will result in products useful to assist the water utilities in the future.

## Introduction

The U.S. Environmental Protection Agency's (EPA) National Homeland Security Research Center (NHSRC) held a Subject Matter Expert Workshop to Identify Cybersecurity Research Gaps and Needs of the Nation's Water and Wastewater Systems Sector on March 30th and 31st, 2016, at the Ronald Reagan Building in Washington, D.C. The purpose of this Workshop was to convene a group of subject matter experts (SMEs) to identify water infrastructure cybersecurity research gaps and needs as recommended by the U.S. Environmental Protection Agency's (EPA) Board of Scientific Counselors (BOSC)[1] (USEPA 2015a). The Workshop was also in keeping with the need identified by the president's National Science and Technology Council (NSTC) in *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security* (NSTC 2016) to gather information concerning state-of-the-art and -technology in cyber defense and response for water and wastewater systems. This research and development strategy identifies areas of research that are needed to help all critical infrastructure sectors defend from, respond to, and recover from cyber-attack.

The information and recommendations provided by the SMEs during this Workshop will be useful to the National Homeland Security Research Center (NHSRC) for developing a better understanding of the impact of cyber intrusion on the water sector[2] and for formulating a research and development approach that will result in products useful to water and wastewater utilities in the future. This Workshop Summary Report provides a high level summary of the 2016 meeting. The SMEs were convened to provide individual advice and recommendations that NHSRC could consider in its cybersecurity research planning efforts. At no point in the meeting were they asked for consolidated, consensus recommendations.

## Background

The nation's awareness of the risks from cyber-attacks and cyber intrusions has been significantly heightened in the last few years. While the impacts of cyber-attacks have been discussed and described as a result of the highly visible breaches in the banking, retail, and entertainment industries, there has been lesser focus on the utility sectors (e.g., water, wastewater, gas, electricity), but that has been changing. In fact, the Water and Wastewater Sector Strategic Priorities Working Group[3] recently identified "cyber events" as one of the *Most Significant Risks*[4] facing water and wastewater systems (DHS, USEPA 2015).

[1] The EPA Board of Scientific Counselors provides advice, information, and recommendations to EPA's Office of Research and Development (ORD) on technical and management issues of ORD's research programs.

[2] Use of the phrase "water sector" is intended to represent the water and wastewater systems sector.

[3] The Water and Wastewater Sector Strategic Priorities Working Group is one of 16 critical infrastructure focused groups organized under the DHS-led Critical Infrastructure Partnership Advisory Council and whose members represent utilities and government organizations.

[4] Risks that need the Water and Wastewater Sector's most urgent attention and greatest resources, based on the pervasiveness of the threat or the potential for high impact. Priority activities should directly mitigate one or more of these risks.

**Water and Wastewater Systems Sector Vision Statement**: *A secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life – assuring the economic vitality of and public confidence in the Nation's drinking water and wastewater service through a layered defense of effective preparedness and security practices in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.*

- **2015 Water and Wastewater Systems Sector-Specific Plan**

The continued and increasing dependency on computer-based systems and networks pervades nearly every aspect of society including how the nation manages much of its critical infrastructure. Cyber-attacks on water utilities can have far reaching impacts on public health; not only in the delivery of clean, potable water to consumers but to other critical services that depend on the continuous delivery of water. As noted in a recent article about water and wastewater process control system[5] (PCS) cybersecurity, "security is important for the water sector because attacks can damage critical infrastructure that affects public safety; lead to significant operational downtime and disruption of service; cause financial loss, such as the loss of revenue for the utility and its customers; and attract significant media attention causing loss of confidence and fear from the public" (Andersen and Phillips 2013). Furthermore, in the interest of cost effectiveness and efficiency, utilities are using remote access and monitoring to operate their control systems via the internet. As described by the Department of Homeland Security (DHS):

> "The nation's critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, *the water we drink* (emphasis added), the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." (https://www.dhs.gov/what-critical-infrastructure)

The reliance on information technology (IT) that underpins the nation's critical infrastructure has also created a relatively new avenue for disruptive attacks against our critical infrastructure.

Although there are similarities between corporate IT systems and water sector PCSs, critical differences exist. These differences are centered on the fact that water sector PCSs are critical systems that must be kept online and continuously running, whereas a corporate IT system can tolerate downtime much more easily and is focused more on the confidentiality and integrity of data. Table 1 highlights the differences between these systems.

[5] Other terms used synonymously include industrial control system (ICS) and distributed control system (DCS).

**Table 1. Differences Between Water Sector PCS and Corporate IT Systems**

| *Water Sector PCS* | *Corporate IT Network* |
|---|---|
| Real time | Not real time |
| Many used for equipment and processes to function | Many used by personnel to create and store data |
| Response time is critical | Consistent response time is desired |
| Rebooting must be scheduled or avoided | Frequent rebooting is acceptable |
| Human safety and process uptime are paramount | Data confidentiality and integrity is of highest importance |
| Generally low bandwidth requirements | High bandwidth requirements |

Source: Andersen and Phillips (2013) InTech Magazine, September/October.

## Federal Role

> "…provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate." (DHS 2013)

While DHS leads the coordinated national effort to manage risks to the nation's critical infrastructure and enhance the security and resilience of America's physical and cyber infrastructure, there are Sector-Specific Agencies (SSA) identified for each of the 16 critical infrastructure sectors. Presidential Directives 7 and 21 designated the EPA as the SSA for the Water and Wastewater Systems Sector. There are many responsibilities assigned to SSAs. A key responsibility relevant to the purpose of this workshop is to "provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate" (DHS 2013).

As the SSA for the Water and Wastewater Systems Sector, EPA works with its partners in identifying, prioritizing, and protecting against threats to water and wastewater systems. EPA shares responsibilities in the mission to protect public health, the environment, and security and resilience activities. While most often the issues facing this sector focus on physical intrusions and damage to various assets, water quality challenges and aging infrastructure, the utilities can, and have been, subject to cyber-attacks and intrusions.

To help all public and private sectors in addressing their cybersecurity risks, the federal government has undertaken various initiatives and assigned federal departments and agencies with public and private sector-specific responsibilities. Executive Order 13636 *Improving Critical Infrastructure Cybersecurity* (2013) calls for the development of a voluntary, risk-based cybersecurity framework—a set of industry standards and best practices to help organizations manage cybersecurity risk. As a result of Executive Order 13636, the National Institute of Standards and Technology (NIST) developed the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) for use across all sectors of the U.S. economy (NIST 2014).

The NIST Cybersecurity Framework is intended to help organizations apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure. The NIST Cybersecurity Framework focuses on using business drivers to guide cybersecurity activities and consider cybersecurity risks as part of the organization's risk management processes. The Framework offers a set of voluntary standards and best practices to help organizations manage cybersecurity risks. The Framework has three parts: the Framework Core; the Framework Profile; and the Framework Implementation Tiers.

The Framework Core consists of five core functions: Identify, Protect, Detect, Respond, and Recover. The Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational profiles. Through use of the profiles, the NIST Cybersecurity Framework is intended to help the utility align its cybersecurity activities with its business requirements, risk tolerances, and resources. The implementation tiers provide a mechanism for utilities to view and understand the characteristics of their approaches to managing cybersecurity risk. As part of its water and wastewater sector-specific responsibilities, EPA is the lead agency to work with this sector to facilitate adoption of the NIST Cybersecurity Framework.

The American Water Works Association's (AWWA) *Process Control System Guidance for the Water Sector* and accompanying Use-Case Tool were designed as a voluntary, sector-specific approach for helping the sector utilities use the NIST Cybersecurity Framework (AWWA 2014). The goal of the AWWA Guidance and Use-Case Tool is to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks. The Use-Case Tool generates a prioritized list of recommended controls based on the specific characteristics of the utility. Users provide information about their PCSs and the manner in which they are used by choosing from a number of predefined use cases. For each recommended control, specific references to existing cybersecurity standards are also provided.

In April 2015, the Critical Infrastructure Partnership Advisory Council (CIPAC) Water Sector Cybersecurity Strategy Workgroup, a joint effort among the water sector and the federal government (co-chaired by EPA), released its *Final Report and Recommendations* in which the workgroup agreed on the need to promote and facilitate the use of the NIST Framework as a way for water system owners and operators to improve their cybersecurity approach.  The most widely used resource to implement the NIST approach is the AWWA Guidance and Use-Case Tool. The workgroup realized that it provides a useful "bridge" from the non-sector-specific NIST Cybersecurity Framework to the water sector-specific user. The workgroup also concluded that in order to increase adoption and use of the NIST Cybersecurity Framework, the water sector needs the following:

- **Increased motivation** to use the NIST Cybersecurity Framework by increasing water sector knowledge of cybersecurity threats and demonstrating the business case (e.g., return on investment) for cybersecurity controls.

- **Enhanced capability** to implement the NIST Cybersecurity Framework through increased technical and implementation support to water sector utilities and increased support to assistance providers.
- **A stronger cybersecurity culture** throughout the water sector that would encourage and support use of the NIST Cybersecurity Framework by embedding it as part of business as usual for utilities by improving the availability of information and lowering the cost of cybersecurity adoption. (CIPAC 2015)

EPA actively coordinates its security and resilience efforts – including cybersecurity issues – with state, local, and Tribal governments and with public and private entities that represent the water and wastewater systems sector (DHS, EPA 2015). EPA also coordinates with DHS to provide insight on the vulnerability and consequence issues that directly impact water and wastewater sector utilities. A better understanding of vulnerability and consequences allows DHS to interpret water-related threat information, and to develop and distribute timely, accurate threat-warning products that are relevant to the sector.

Most recently, as part of the President's *Cybersecurity National Action Plan* (The White House 2016), the *2016 Federal Cybersecurity Research and Development Strategic Plan* was released (NSTC 2016). This updates 2011's *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program* (NSTC 2011). With the goal of making cyberspace inherently more secure, the plan challenges the cybersecurity research and development community to provide methods and tools for deterring, protecting, detecting, and adapting to malicious cyber activities. The plan defines near-, mid-, and long-term goals to guide and evaluate progress.

In August 2015, the EPA's BOSC Homeland Security Subcommittee conducted its first annual review of the Agency's Homeland Security Research Program (HSRP). The purpose of this review was to assess the nature and direction of the research and to help address the question "Is the Office of Research and Development (ORD) doing the science right?" Among the numerous recommendations, the Subcommittee offered the following concerning cybersecurity-related research and development:

> "Because of the severity of the threat of cyber-attacks, the research schedule should be modified to prioritize cyber security research ahead of other areas to counter the continuous and ever-increasingly [sic] sophistication of cyber-attacks that plague utilities. As utilities interconnect formally [sic] disconnected systems to increase efficiencies, they create an ever expanding attack surface – often without understanding the impact and risks. As very few utilities have staff prepared to deal single-handedly with chemical or biological attack remediation, knowledge of cyber security is limited in the utility space; consequently research and guidance is needed from HSRP."

The cyber threats are a real concern to the water industry. Therefore, EPA needs the assistance of private and public sector cybersecurity and water and wastewater utility experts to more fully comprehend the cybersecurity research gaps and needs. The important insights of the SMEs assist the Agency in making an informed assessment concerning the direction of cybersecurity research.

## Workshop Organization

Eleven SMEs from outside the Agency were invited to participate and provide input; another 24 stakeholders participated as observers (Appendix A). The stakeholders and SMEs represented water and wastewater utilities, water trade and professional associations including consultants that have supported water utilities in cybersecurity, water associations and research organizations, and staff from a DOE National Laboratory (Table 2). In addition, staff from DHS and EPA also participated in the workshop.

**Table 2. Organizations Represented by the Participants**

**Water Utilities**

Washington Suburban Sanitary Commission
United Water
Las Vegas Valley Water District
Massachusetts Water Resources Authority
DC Water and Sewer Authority
Fairfax County Water Authority

**Industry Representatives**

Booz Allen Hamilton
Arcadis
EMA
Black & Veatch

**Federal Organizations**

*Department of Homeland Security*

Homeland Security Advanced Research Projects Agency (HSARPA)

National Cyber and Communications Integration Center – Industrial Control System Cyber Emergency Response Team (NCCIC, ICS-CERT)
National Cybersecurity Assessment & Technical Services (NCATS)

*Environmental Protection Agency*

Office of Groundwater and Drinking Water, Water Security Division
Office of Wastewater Management
Office of Research and Development, National Homeland Security Research Center
Office of Research and Development, Office of Scientific Information Management

*Department of Energy*
Idaho National Laboratory

**Non-Governmental Organizations**

American Water Works Association (AWWA)
WaterISAC (Water Information Sharing and Analysis Center)
Water Research Foundation (WRF)

To facilitate discussions about cybersecurity research gaps and needs, the workshop deliberations were divided into three mutually supportive sessions: cyber risk assessment, cyber risk management, and a closing session that was used to discuss identified research gaps and needs. The agenda is provided in Appendix B.

Each of the first two sessions were driven by some specific charge questions that were sent out in advance and used to elicit discussion. The first session focused on the subject of *cyber risk assessment*. The charge questions for this session were:

- How can we describe the current and future cyber risks facing the water sector?
- Considering these risks, how do we best inform decision making in the water sector for—
    - the range of communications currently being used (e.g., Internet, telephone wires)?
    - the capacity differences among small, medium and large-to-very-large systems?

The second session provided a forum for discussion on *cyber risk management*. The charge questions for this session were:

- Are there cybersecurity tools developed for other sectors (e.g., electrical power grid, oil/gas pipelines) that could be adapted for use by the water sector?
- What are the emerging technologies that could be applied to the water sector's risk? Are there vendors solely focused on the water sector's cybersecurity needs?

In preparation for the third and closing session, the SMEs were asked a few weeks in advance of the workshop to identify potential high-priority cybersecurity research gaps and needs and to make prioritized recommendations for which needs most urgently needed research. Input was received from most of the SMEs. The various inputs were combined into a single list that was distributed back out to the SMEs prior to the meeting so they could see what their colleagues identified and to allow them to prepare for the closing session discussion. The SMEs provided 49 recommendations focused on protection of water infrastructure components and systems from cyber-attack and to insure confidentiality, integrity, and accountability of the PCS (Appendix C).

It was observed during the sessions that the discussions did not always stick to the theme of the session and, in fact, there did not seem to be a clear demarcation between approaches and research gaps that support cyber risk assessment and those that address cyber risk management. The following narrative contains the general nature of the SME discussions in that it describes the current and emerging cybersecurity risks facing the water and wastewater utilities, but also captures the salient points, sometimes in the form of a possible "fix", suggested by the SMEs during the discussion. Therefore, the report summarizes the discussions by key topic area.

## Water Sector Cybersecurity Concerns

Cybersecurity problems facing the water and wastewater sectors are multifaceted, ranging from situational awareness about the possibility of cyber-attacks to recovery from cyber-physical intrusions into PCSs. The breadth of these problems illustrates the wide range of issues facing water utilities when considering cybersecurity.

### Information Technology/Operational Technology (IT/OT) System Architecture

IT and OT departments within the utilities generally have different structures and cultures. The SMEs acknowledged this difference and the lack of operation best practices and effective communication between these two departments.

The SMEs recognize that while many vulnerabilities are known, there are constant efforts by individuals with both good and bad intent to find and exploit new ones. The challenges are growing for the utilities because they are being pushed to increase their efficiency and to reduce costs by enhancing connectivity, thereby increasing the risk of exposure to malicious attack.  And furthermore, the once segregated information technology (IT) and operational technology (OT) systems are sometimes being merged into a single, internet-facing network which adds additional complexity and cyber risk to the utility operations.

IT and OT: What's the difference?

**Informational Technology (IT)** is key to running the business side of a utility – it keeps the information flowing, email running, and databases populated. **Operational Technology (OT)** describes the collection of hardware and software that is used to keep an industrial process, such as the production and distribution of water, running. It often includes the supervisory control and data acquisition (SCADA) system.

Yet another challenge is that many utilities rely on the Windows operating system as the backbone for their IT and OT environments. Historically, the Windows operating system has been the most obvious choice for use as the primary PCS building block.  Thus PCS software remains almost exclusively dependent on it. Windows platforms are difficult to replace. In one example provided, an SME found that he was coming across PCSs that are still relying on Windows 95 -- a very old and highly exploitable version of Windows that is no longer supported by Microsoft. The IT and OT staff must be cognizant of the known vulnerabilities (and have patched vulnerable systems) and understand that zero-day vulnerabilities appear regularly and, until patched, provide new avenues of cyber-attack.

What is network segmentation?

Network segmentation is the practice of dividing a computer network into functional subnetwork zones . Advantages of such splitting are primarily for boosting performance and improving security. If a cyber-criminal gains unauthorized access to a network, segmentation can impede the attacker's access to other parts of the network.

Because of these issues, the SMEs agreed that ensuring that the IT and OT systems are properly segmented is very important particularly as the perimeter of the supervisory control and data acquisition (SCADA) system can be very large and extend beyond the physical boundary of the plant walls and fences.

## Cyber-Physical

SMEs also recognized that the cyber-physical aspects of cybersecurity present a significant challenge. It is important to note that there are utilities with OT assets in remote locations (e.g., a pumping station outside the confines of the main utility location) that are more vulnerable to physical attack. This means that an OT device could be compromised either by physical damage or by some means of attack to the computer/process networking capability of the asset after it is physically contacted. Tampering with remotely located equipment may also provide a means for entry (a “backdoor” of a fashion) into the SCADA system. However, the SMEs agreed that it is more likely that an attacker will sit behind a keyboard tens, hundreds, or thousands of miles away and utilize a known exploit (or multiple exploits) to gain access to a system rather than go to a remote pumping plant, break into it, and then physically connect a computer to the programmable logic controller (PLC) or remote terminal unit (RTU). However, physically securing devices in locking cabinets with intrusion detection sensors is being implemented by many utilities as a means to minimize the ease with which someone could tamper with a device.

A few SMEs noted that identifying potential process impacts (e.g., damaging pumps or pipes) helps to identify weak spots in the system to pinpoint locations where security improvements could be made (e.g., installing timers for restarting pumps). A number of the utilities have installed safety systems external to the PLC to protect it from potential attack impacts. Clearly, preventing damage to key pieces of equipment is necessary to ensure that a water or wastewater system is not taken entirely offline to repair or replace the damaged device. Water and wastewater utilities provide essential health and safety functions in a community, so protecting all components comprising the system, and identifying the weakest link is of extreme importance.

It was pointed out that Industrial Control System Cyber Emergency Response Team (ICS-CERT) has cause to look at and investigate a wide range of cyber-attacks and the underlying vulnerabilities and it has given it a really good handle on what is out there. ICS-CERT starts its investigation and assessments at the hardware comprising a PCS (i.e., PLCs, RTUs, HMIs) but not at the processes themselves. SMEs suggested that vulnerability assessments should go beyond the current ICS-CERT approach which stops at the PLC. The risk was framed in the form of a question “If someone actually accessed a control system, could the damage they cause create a widespread impact?” Cyber risks tend to be looked at in a piecemeal fashion, often at the utility level and not holistically, which makes managing the risks and responding to intrusions all the more difficult.

## Communications

The water sector's critical infrastructure depends on telecommunications systems for command and control functions, resulting in the migration of these critical infrastructure systems to new communication technologies. As such, common communication protocols and open architecture standards have begun to replace the distinct proprietary mechanics of PCSs. Although this has had positive impacts, the replacement also introduces vulnerabilities and new risks to these systems (DHS 2009).

In addition, as PCSs move more toward automation and remote access, the manual operation of systems as a fallback position in an emergency is becoming more difficult for a couple of reasons. First, there is a gradual loss of personnel experienced in manual operation of the system and, second, the design of newer plants does not necessarily provide easy access to valves and other operating control devices.

The SMEs discussed emerging risks during the meeting, noting that telecommunications providers are phasing out hard-wired systems and moving toward wireless communication. It is becoming more difficult and expensive to maintain a hard-wired telecommunications capability as a backup, and the wireless communication platforms are more difficult to protect from attacks (i.e., signal jammers and hacking wireless communications). The increasing cost of effective telecommunication solutions increases the risks and vulnerabilities of systems of all sizes. In addition, one of the ICS-CERT representatives has noticed that utilities are increasing the use of remote access of pumping stations and monitoring locations but secure implementation is somewhat lacking. The transition from serial-based communication with PCS devices to network-based communication is increasing the SCADA "perimeter" beyond the traditional, "behind the fence" perimeter, as Ethernet and wireless connection to remote locations becomes more prevalent. This desire to remotely access and manage utility processes puts greater emphasis on the need to protect systems from attack by using network hardware appliances such as data diodes (a unidirectional gateway) and enterprise-level firewalls to create as many barriers to would-be hackers as possible. However, enterprise firewalls and data diodes do not protect master stations from field device hacking. While these are good practices, they are insufficient. Good patching practice, good local access controls, and good field device physical security are fundamental to managing the overall security of a system.

## Hardware and Software

Monitoring software tools and approaches were discussed. These discussions addressed the use and availability of open source software tools (e.g., WireShark, Nmap, Bro Network Security Monitor, and tcpdump, to name a few) that are widely used in penetration testing and which could also be used to monitor network traffic. However, a number of the SMEs cautioned that the use of these tools on an OT network might be problematic because the devices used in an OT architecture may not be able to handle the digital "overhead" associated with the use of the tools. It was also pointed out that in addition to open source software there are a few commercial products available to utility managers.

These include Sophia™, Thetaray, and Splunk®. However, the SMEs cautioned that a significant amount or training is necessary to fully utilize the many tools available and that few utilities have the luxury of sending their staff to the necessary specialized training.

SMEs pointed out that it has been very challenging to get technology vendors to do a better job of building security features into their components. There has been little incentive for them to do so, but, as one SME mentioned, Underwriter's Laboratories (UL) recently stood up its UL Cybersecurity Assurance Program (UL CAP) that will certify (through extensive, hands-on evaluation) the security of network-connectable devices and systems as well as the vendor processes for developing and maintaining these devices and systems. It is based on its recently promulgated cybersecurity standard UL 2900-2-2 *Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems*. UL CAP has only recently started evaluations, but, as one SME pointed out, this could be an important start in hardening devices used in PCSs.

## Regulatory and Industry Standards

It was also noted that there are no required minimum cybersecurity standards applicable to the water and wastewater utility sectors as there is for the electric power sector[6]. It was pointed out by one SME that in the electric industry the utilities were driven to a "security by compliance" mode of operation which had the effect of decreasing cybersecurity protections. The regulations established the minimum acceptable performance requirements which utilities are compelled to meet, but not necessarily exceed. So if new software or hardware entered the market that could be used to exceed the cybersecurity performance requirements, they were not being procured because the utilities were already in compliance with the current requirements. None of the SMEs, AWWA, nor the Agency were advocating for the creations of a similar set of regulatory or otherwise enforceable standards for the water and wastewater utility sectors. However, it was simply noted that it has been challenging for water and wastewater utilities to employ systems and technologies that protect the IT and OT assets from cyber-attack given all the other responsibilities they have.

Workshop attendees acknowledged that there are some standards and tools available to the water industry to help assess cyber risk. For example, ICS-CERT offers its Cyber Security Evaluation Tool (CSET) to assist utilities in either conducting a self-assessment or to work with the ICS-CERT staff to conduct an on-site assessment. In addition, the AWWA J100-10 (R13) Risk and Resilience Management of Water and Wastewater Systems (RAMCAP) (AWWA 2010) methodology was created explicitly for the water and wastewater sectors. While CSET is specific to cybersecurity risk assessment across all sectors, J100 it

[6] In 2007, the Federal Energy Regulatory Commission (FERC) designated North American Electric Reliability Corporation (NERC) the Enterprise Reliability Organization (ERO) in accordance with Section 215 of the Federal Power Act, enacted by the Energy Policy Act of 2005. Upon FERC's approval, NERC's Reliability Standards became mandatory within the United States. These mandatory Reliability Standards include critical infrastructure protection cybersecurity standards (CIP) which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States.

more broadly focused guidance for calculating the probability of a specific natural hazard occurring at a given utility (i.e., earthquake, tornado, and hurricane). There was some discussion about the inclusion of a cybersecurity component being added to J100 sometime in the future.

Additionally it was noted that the AWWA has been actively engaged in supporting the cybersecurity needs of water utilities separate from J100, first through its involvement in the development of the *Roadmap to Secure Industrial Control Systems in the Water Sector* (WSCC CSWG 2008) and most recently having created its *Process Control System Security Guidance for the Water Sector* (AWWA 2014) and the supporting Use-Case Tool which were specifically designed to provide water sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyber-attacks. This AWWA resource is designed to provide actionable information for utility owner/operators based on their use of PCSs.

## Issues Impacting Cybersecurity Management

SMEs acknowledged that no utility will be able to protect against or mitigate every cyber risk. Therefore, completing a cyber-assessment within the framework of an overall risk equation (i.e., not separating out cybersecurity) is important and will help utility management support an organization's cybersecurity efforts. To address cybersecurity issues, it is necessary for decision makers to take into account physical security, technology, and administrative issues as a whole, establishing a culture that not only includes cybersecurity and technology experts, but also human resources personnel and line managers. As the knowledge of cybersecurity risk and mitigation improves, decision makers within organizations can make more informed decisions on how to best invest their money in cybersecurity architecture that will reduce cybersecurity risks. SMEs acknowledged that research is needed to develop some cybersecurity performance specifications that decision makers could consider when assessing their cybersecurity needs to best protect their utilities, systems, and customers.

The SMEs were all familiar, for the most part, with the NIST Cybersecurity Framework and the AWWA Guidance and Use Tool. While the Framework provides some good, solid guidance to the utilities, there was a very lively discussion concerning cyber security risk management issues facing the water and wastewater sector and what it means to actually implement approaches to manage the risk. It was clear from the discussion that managing cyber risk is similar to a war being fought on many fronts. There are:

- personnel issues (training, expertise, certification, and integrity),
- hardware capabilities and vulnerabilities,
- software capabilities and vulnerabilities, and
- issues concerning the physical protection of the utility's assets.

A significant concern facing the utilities is the decreasing number of qualified and experienced operators. Utilities are facing additional pressure because of the decreasing number of operators at the utilities as the use of automation grows. Larger utilities are often no longer able to operate without a SCADA system in place. While the move to a more automated system will have direct impact on improving efficiency and the financial bottom line, reliance on automation also exposes utilities to more cyber risk. It was noted by the SMEs that utilities need to plan better for a SCADA system shut down, attack, or crash.  One of the SMEs pointed out that his utility annually shuts down all of its PLCs and operates the system manually to ensure they know what to do in the event of a SCADA system outage. Plans for manual operation, including possible sharing of operators using a WARN (Water and Wastewater Agency Response Network) agreement among nearby facilities, are needed if SCADA systems fail. Such operational suggestions were discussed throughout the workshop but are not captured in any significant detail in this report because they are not research needs.

There was considerable discussion about the human element, beyond the need for skilled operators, in cybersecurity. The willful or unintentional actions of utility staff can be a vulnerability that cannot be fixed with a “patch” or a network appliance. The human element in cybersecurity is at least as important to the IT and OT parts of the operation as are appropriately hardened network appliances. Clearly, various types of training and guides are available to utilities to help them inform their staffs about general cybersecurity measures (e.g., use strong passwords) to very complex training that introduces the IT and OT staff to the intricacies of PCS design, operation, and management (e.g., Cyber Security Industrial Control Systems 210W coursework series [ICS-CERT]). However, it is important for the utilities to fully vet the background of its employees to ensure that, to the extent possible, their staff will not be the source or cause of a cyber intrusion and the possible shutdown of their system.

Another sizable issue expressed by the SMEs was the level of awareness about the importance/impact of cybersecurity among the executive leadership in a utility and how to help raise that awareness. They felt that additional effort needs to be made to reach out to executives to clearly demonstrate the impact that a cyber-attack could have on the utility and the people it serves. One SME pointed out that once his General Manager “got it” and made cybersecurity his number one priority, everything changed for the better at his utility. The executive leadership sets the tone for the whole organization. Therefore support by the leadership will help the IT and OT managers to convince their senior management that allocating the staff time necessary to attend training or take an online class would give them a good return on investment.

There was a long discussion by the SMEs about the advantages of some type of a certification program, an incentive program, or some other form of recognition along the lines of NIST’s Malcolm Baldrige National Quality Award, to help utilities prioritize cybersecurity needs funding within the budget planning for the utility[7]. The SMEs also acknowledged the difficulty in crafting these programs as there is no “one size fits all” approach. While interesting, the nature of the discussion was outside the scope of this workshop.

[7] On July 12th, 2016 NIST announced the Baldrige Cybersecurity Initiative to complement the NIST Cyber Security Framework. More information can be found at: http://www.nist.gov/baldrige/enter/baldrige-cyber.cfm.

### Utility Size and Business Model

SMEs agreed that the size of the population served by a utility has a direct impact on the capability of the utility to focus on and deploy cybersecurity measures, yet all utilities, regardless of size have the same cyber risk. Smaller systems, in general, do not have the same staff and financial resources available to them as larger utilities. The SMEs noted the importance of finding ways to reach the operators of the smaller systems with the appropriate and necessary guidance. The smaller utilities need additional assistance to help them get the "biggest bang for their buck" when assessing cyber risk and implementing cybersecurity measures. The SMEs noted how important it is to establish communication mechanisms with small systems, which do not have the available funds to attend meetings, conferences, or workshops about cybersecurity. Additionally, the capacity of the utility determines the appropriate actions and solutions that should be taken to protect itself from cyber-attack. Finally, SMEs noted that in addition to differences in capacity, many different organizational structures (publicly or privately managed) exist in water utilities across the country, and this too will have an impact on effectively managing risk.

### Training and Education

Cybersecurity training and education needs were frequently raised during the workshop. There were few cybersecurity issues raised during the discussions where a training or education need was not expressed. The SMEs were, for the most part, aware of the extensive assortment of training available from EPA, AWWA, and ICS-CERT. It was pointed out to the SMEs that while training and education needs were duly noted, addressing them is outside the realm of the technology-based cybersecurity research and development theme of the workshop. A couple of examples of available training were noted during the discussion including the one-day water cybersecurity outreach and training workshops that were supported by the EPA Office of Water's Water Security Division in conjunction with local utilities throughout the country (www.horsleywitten.com/cybersecurity/) and the variety of free (online or instructor-led) courses dealing with operational security, PCSs, and hands-on exercises available from ICS-CERT (ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT).

## Sessions Summary

As mentioned previously, the overarching purpose of the workshop was to enlist the help of the SMEs to identify and prioritize areas of research that are needed to help the water sector defend from, respond to, and recover from cyber-attacks. All the SMEs agreed that there are many cybersecurity challenges facing the water sector and, as one SME pointed out, that in addition to the many challenges, most utilities are "customized" with regard to the design and operation of the IT and OT networks which makes it difficult or even impossible to come up with a "one size fits all" approach to cybersecurity. This uniqueness adds more challenge to the risk assessment and management processes.

Table 3 captures the water sector cybersecurity risks and issues discussed during the two previous sessions as well as in the pre-workshop recommendations. Eight out of the 11 SMEs (five water utility representatives and three industry consultants plus one federal national laboratory representative) provided 49 recommendations prior to the Workshop (Appendix C). The majority of the recommendations focused on ways to protect the components and systems from cyber-attack and to ensure confidentiality, integrity, and accountability of the PCSs. This included suggestions on encouraging recognition of cybersecurity problems at the management level and the sharing of technical information about cybersecurity technologies that are being used successfully at some utilities. A number of the recommendations focused on SCADA and/or PCS related issues. It was not surprising that much of the discussion during the first two sessions emphasized the importance of defending the PCS from cyber-attack. There were a few recommendations that either addressed possible ways to discourage malicious cyber activity or ways to detect whether a system has been breached.

**Table 3. Water Utility Cybersecurity Risks and Issues**

**OT and IT System Architecture**

- IT/OT systems are unique/custom
- IT/OT systems are most often managed separately
- There are challenges with effectively segmenting IT and OT networks (particularly when using a common broadband connection)
- Many systems are not regularly patched which allows known and zero-day vulnerabilities to be exploited
- Regular monitoring is not routinely implemented to ensure that malicious content is not being introduced to networks

**Cyber-Physical**

- Available hardware appliances (e.g., firewalls, intrusion detection systems, data diodes) require specialized knowledge and training to use properly
- Enhanced physical devices (e.g., locks, fences, barricades, key management, surveillance) need to be regularly updated and managed
- This sector must manage remote facilities and operations as part of service delivery

**Communications**

- Wireless telecommunications have known issues that must be managed
- Numerous, traditionally used communication protocols with security issues need to be managed and, when appropriate, replaced
- Remote system access is being relied upon more extensively but it creates more opportunity for exploitation
- The SCADA perimeter is expanding and with it comes new protection problems

**Hardware and Software**

- Some utilities may not make use of existing software tools to conduct basic hygiene monitoring
- Some form of cybersecurity performance (system and individual) certification is needed
- Update and expand the type and availability of cybersecurity training

**Table 3. Water Utility Cybersecurity Risks and Issues**

- Insist on more attention to cybersecurity in design (influence vendors by imposing stricter security requirements as a condition of procurement)
- Proprietary nature of SCADA system designs makes a “one size fits all” solution impractical
- “Lightly configured” devices that continue to be used with default access mechanisms wide open thereby providing easy malware access to systems.

**Regulatory and Industry Standards**

- Lack of legal authority and assignment of responsibilities for accountability
- Vulnerability assessments not inclusive enough to identify issues
- Cyber risk is approached in a piecemeal fashion across various guidance, policies, and frameworks

**Water Utility Cyber Risk Management**

- Cyber risk awareness is lacking
- Importance of having cybersecurity plans in place
- Utility resistance to changing, modifying, and replacing PCSs (i.e., choosing familiarity over security)
- Lack of education and knowledge of risk at all levels in the utility, but the executive leadership level is probably the most critical
- Employee background checks needed to thoroughly vet staff

**Utility Size and Business Model**

- Small systems need additional technical, managerial, and financial support
- Lack linkages/communication with larger utilities or support organizations
- Public, private, investor owned risk management variable

**Training and Education**

- OT operators need specialized training (e.g., OT operator certification)
- More training opportunities needed and that are well publicized

Throughout the meeting, the SMEs recognized that some of the pre-meeting recommendations they provided were either ongoing and/or outside the realm of the cybersecurity research and development goals targeted by this workshop. For example, some of the pre-meeting SME recommendations raised issues pertaining to the classification of labor positions and compensation packages for water sector cybersecurity professionals, general insurance or bonding for water utilities, and a rating or certification system for ICS product vendors.

There also was agreement that some of these research recommendations were applicable to a number of sectors beyond the water sector, and EPA was encouraged to reach out and pursue collaborations with other government agencies and critical infrastructure sectors to address these recommendations.

The SMEs felt that the following potential projects would merit consideration and interest outside of EPA:

- Software and firmware patch repository for ensuring integrity of patches and easy access by the utilities.
- Developing a clearer understanding of the security implications of using cloud services to support utility operations (e.g., energy management and water quality tracking).
- Develop and test a standardized procedure for configuring servers used to manage process control.
- Establish a security rating system for OT providers and a system to rate the "package panels" that are routinely used in utilities.

## Top Priority Water Sector Cybersecurity Research Gaps

The purpose of the closing session was to draw from the previous two discussion sessions and the pre-meeting recommendations to identify the highest priority research needs. This final session was used as an opportunity to revisit and discuss some of the earlier identified gaps and needs and to return to the list of cybersecurity research and development recommendations that the SMEs provided prior to the workshop. To aid the SMEs and to facilitate discussion, the NHSRC consolidated the list into a single table of 24 recommendations.

The SMEs worked through the list of 24 recommendations and winnowed it down to 15 (Appendix D). These 15 recommended needs were subsequently ranked individually by the SMEs after the workshop and then NHSRC consolidated the submissions to create a final list of the research gap recommendations that are relevant to the NHSRC mission (Table 4).

**Table 4. Top-Priority Water Sector Cybersecurity Research Gaps and Needs Recommended by the Subject Matter Experts**

**1. Cyber/Physical Impacts and Design Mitigations**

Foster a better understanding of the operational and physical impacts of a cyber-attack on water and wastewater systems among utilities, water industry trade associations, and government policymakers. Consider addressing questions such as "Can an attacker maliciously operate pumps to failure, break mains, cause discharge violations, or create long-term production outages?" If so, "What are the cyber exploits needed to cause these impacts?" "Are there PCS design modifications that could mitigate or prevent these impacts?" Research avenues to consider:

- ➢ Develop case studies of successful drinking water and wastewater systems and their reorganization to meet the need of better cyber and physical security.  This can lead to information that may help the EPA Office of Water and AWWA develop best practices guidance.

**Table 4. Top-Priority Water Sector Cybersecurity Research Gaps and Needs Recommended by the Subject Matter Experts**

- Demonstrate how a water pump could be damaged or destroyed via cyber-attack (akin to ICS-CERT's Aurora demonstration wherein a large electrical generator was destroyed via cyber-attack).
- Testing and evaluation of representative water infrastructure equipment with eye toward how cyber-hardened they are (security by design or as an afterthought)
- Water infrastructure mitigation techniques on how utilities can install low cost SCADA – independent safety systems that can protect physical infrastructure from being damaged by malicious acts of a hacked SCADA system - develop 'best-practices" information
- Evaluate whether existing water/wastewater system hydraulic models could be modified to include PCS monitoring and energy use data to provide another means of detecting when a cyber intrusion occurs.
- Exercising and exploring vulnerabilities in OT network architecture (includes hardware and software) to assess difficulty in accessing and attacking key points in the overall PCS (with the intent to do harm).

**2. IT/OT Software and Monitoring Design**

Water utilities need information and guidance on the availability, use, and quality of open source software. NHSRC could conduct testing of devices to determine how effective they are at providing additional cybersecurity protections. Link network monitoring (IT) software with water infrastructure (OT) software.

- Compile a package currently available network monitoring tools into a software suite.
- Test and evaluate network "hygiene" monitoring tools.
- Develop an approach for utilities to test and evaluate software and/or devices pre-deployment using a testing environment that isolates (also known as "sandbox") them from the production environment.
- Network defense hardware appliance testing to include, for example, firewalls and intrusion detection systems.
- Provide guidance on understanding the advantages of segmenting (e.g., air-gapping) a utility's computer network

## Conclusions

Modern water and wastewater facilities are using SCADA systems and/or PCSs to automate their management, treatment, and delivery of services. In the past, PCSs were reasonably well isolated from the internet because the PCS architecture and equipment were unique to process control and were operated outside of commonly recognized IT environments. However, over the last several years, the PCS equipment design and operation has taken advantage of the less costly network-based (IT) computing environment that had typically been reserved for the business side of the utility operation. As a result, the OT and IT systems are being merged at many utilities. In addition, in the interests of efficiency and cost-effectiveness, many utilities are relying more and more on internet-facing SCADA and/or ICS systems for ease of management through remote access.  This evolution in OT network design and management causes an increase in the cyber-attack surfaces of a utility and potentially increases the risk of cyber intrusion. Cybersecurity challenges facing the water and wastewater sectors are multifaceted, ranging from situational awareness about the possibility of cyber-attacks to recovery from cyber-physical intrusions into a PCS. The breadth of these concerns illustrates the wide range of issues facing water utilities when considering how to manage cyber risks and to recover from a successful cyber-attack.

The SMEs invited to participate in the workshop brought important perspectives, insights, and actual experiences into the day-and-a half discussions about cybersecurity issues facing water and wastewater utilities. As a result, NHSRC gathered important information about PCS operation and the corresponding cybersecurity needs of water and wastewater utilities. It is clear from the discussions that the utilities have many needs ranging from cybersecurity staff training to the development and deployment of currently available and new software and hardware tools and devices.

## Next Steps

As a key next step following the workshop, NHSRC anticipates forming productive collaborations and partnerships with other government agencies, drinking water and wastewater utilities, and nongovernmental organizations in conducting research and development projects relevant to the cybersecurity needs of the nation's water sector. This workshop was an important first step in the process of identifying potential research areas and partners. NHSRC, along with its Office of Water partners, will continue to discuss the feasibility of adding cybersecurity-related research efforts to the Agency's Homeland Security Research Program.

# References

American Water Works Association. 2010. *AWWA J100-10 (R13): Risk and Resilience Management of Water and Wastewater Systems (RAMCAP).* Denver, CO: AWWA.

American Water Works Association. 2014. *Process Control System Security Guidance for the Water Sector*. Denver, CO: AWWA. Accessed December 14, 2016, www.awwa.org/Portals/0/files/legreg/documents/AWWACybersecurityguide.pdf

Andersen, N., and Phillips, B. 2013. "Water and Wastewater SCADA Cybersecurity." *InTech Magazine*. September/October. Accessed December 14, 2016, www.isa.org/standards-and-publications/isa-publications/intech-magazine/2013/september/web-exclusive-water-and-wastewater-scada-cybersecurity/

Critical Infrastructure Partnership Advisory Council. 2015. *Final Report and Recommendations*. Washington, D.C.: CIPAC Water Sector Cybersecurity Strategy Workgroup. Accessed December 14, 2016, www.awwa.org/Portals/0/files/legreg/security/CyberCIPACFinalReport2015.pdf

Department of Homeland Security. 2009. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*. Washington, D.C.: DHS, Science and Technology Directorate, National Cyber Security Division, Control Systems Security Program.

Department of Homeland Security & U. S. Environmental Protection Agency. 2015. *Water and Wastewater Systems Sector-Specific Plan*. Washington, D.C. Accessed December 14, 2016, https://www.dhs.gov/publication/nipp-ssp-water-2015

Department of Homeland Security. 2013. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, DC. https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf

Executive Order No. 13636, 78 C.F.R. 11737 (2013)

National Institute of Standards and Technology. 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: NIST. Accessed December 14, 2016, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Science and Technology Council. 2011. *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program.* Washington, D.C.: National Science and Technology Council. Accessed December 14, 2016, www.whitehouse.gov/sites/default/files/microsites /ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

National Science and Technology Council. 2016. *Federal Cybersecurity Research and Development Strategic Plan: Ensuring Prosperity and National Security*. Washington, D.C.: NSTC Networking and Information Technology Research and Development Program. Accessed December 14, 2016, www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf

The White House. 2016. Cybersecurity National Action Plan. Accessed December 14, 2016, https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

Underwriters Laboratories. 2016. Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems. Standard UL 2900-2-2. Accessed December 14, 2016, http://ulstandards.ul.com/standard/?id=2900-2-2

U. S. Environmental Protection Agency. 2015a. *Draft Report of the EPA Board of Scientific Counselors Homeland Security Subcommittee*. Cincinnati, OH: EPA Board of Scientific Counselors.

Water Sector Coordinating Council Cyber Security Working Group (WSCC CSWG). 2008. *Roadmap to Secure Control Systems in the Water Sector*. Sponsored by AWWA and DHS. Accessed December 14, 2016, http://www.awwa.org/Portals/0/files/legreg/Security/SecurityRoadmap.pdf

The White House. 2016. Cybersecurity National Action Plan. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

# APPENDIX A
## Workshop Participants

**Utility Representatives**

**Jake Brodsky**
Washington Suburban Sanitary Commission
14501 Sweitzer Lane
Laurel, MD 20707
E-mail: jake.brodsky@wsscwater.com

**Ed Hackney**
United Water, Inc.—SUEZ ENVIRONNEMENT
461 From Road
Paramus, NJ 07652
Telephone: (201) 767-9300
E-mail: ed.hackney@suez-na.com

**Gregory Hearn**
Las Vegas Valley Water District
Information Technology Department
Administration and Infrastructure
1001 S Valley View Boulevard
Las Vegas, NV 89107
Telephone: (702) 258-3100
E-mail: greg.hearn@lvvwd.com

**Andrew Hildick-Smith**
Massachusetts Water Resources Authority
Emergency Planning and Preparedness
Charlestown Navy Yard
100 First Avenue, Building 39
Boston, MA 02129
Telephone: (617) 305-5628
E-mail: andrew.hildick-smith@mwra.com

**Diana McCormick**
District of Columbia Water and Sewer Authority
Process Control System & Supervisory Control and
Data Acquisition
5000 Overlook Avenue, SW
Washington, DC 20032
Telephone: (202) 787-7132
E-mail: diana.mccormick@dcwater.com

**Sonny Ngo**
Fairfax County Water Authority
8570 Executive Park Avenue
Fairfax, VA 22031
Telephone: (703) 289-6521
E-mail: vngo@fairfaxwater.org

**Augustin Serino**
Massachusetts Water Resources Authority
Emergency Planning and Preparedness
Charlestown Navy Yard
100 First Avenue, Building 39
Boston, MA 02129
Telephone: (617) 305-5812
E-mail: augustin.serino@mwra.com

**Nongovernmental Organization Representatives (Associations)**

**Michael Arceneaux**
Water Information Sharing and Analysis Center
1620 I Street, NW
Washington, D.C. 20006
Telephone: (202) 331-0479
E-mail: arceneaux@waterisac.org

**Kevin Morley**
American Water Works Association
1300 I Street, NW, Suite 701W
Washington, D.C. 20005
Telephone: (202) 326-6124
E-mail: kmorley@awwa.org

**Chris Rayburn**
Water Research Foundation
6666 W Quincy Avenue
Denver, CO  80235
Telephone: (303) 347-6188
E-mail: crayburn@waterrf.org

**Industry Representatives (Consultants)**

**Philip Gaberdiel**
EMA, Inc.
1001 Morehead Square Drive, Fifth Floor
Charlotte, NC  28203
Telephone: (704) 375-0123
E-mail: pgaberdiel@ema-inc.com

**Daniel Groves**
Arcadis
410 N 44th Street, Suite 1000
Phoenix, AZ  85008
Telephone: (602) 241-1770
E-mail: daniel.groves@arcadis.com

**Christian Manalo**
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA  22102
Telephone: (703) 377-1697
E-mail: manalo_christian@bah.com

**Shannon Spence**
Arcadis
44 S Broadway
White Plains, NY  10601
Telephone: (914) 641-2443
E-mail: shannon.spence@arcadis.com

**Federal Agency Representatives**

**Michael Carpenter**
Idaho National Laboratory
Environmental Engineering & Technology
2525 Fremont Avenue
Idaho Falls, ID  83415
Telephone: (208) 526-8467
E-mail: michael.carpenter@inl.gov

**Ron Fisher**
Idaho National Laboratory
Homeland Security Division
2525 Fremont Avenue
Idaho Falls, ID  83415
Telephone: (208) 526-5630
E-mail: ron.fisher@inl.gov

**Chase Garwood**
U.S. Department of Homeland Security
Department of Science and Technology
Homeland Security Advanced Research Projects Agency
3801 Nebraska Avenue, NW
Washington, D.C.  20016
Telephone: (202) 282-8000
E-mail: chase.garwood@hq.dhs.gov

**Robert Timpany**
U.S. Department of Homeland Security
Idaho Chief of Operations
Industrial Control System Cyber Emergency Response Team
National Cyber and Communications Integration Center
2525 Fremont Avenue
Idaho Falls, ID  83415
E-mail: robert.timpany@hq.dhs.gov

**Scott Tousley**
U.S. Department of Homeland Security
Department of Science and Technology
Homeland Security Advanced Research Projects Agency
3801 Nebraska Avenue, NW
Washington, D.C.  20016
Telephone: (202) 254-5714
E-mail: scott.tousley@dhs.gov

**Kenneth Vrooman**
U.S. Department of Homeland Security
National Cybersecurity Assessments and Technical Services
500 C Street, SW, Room 404B
Washington, D.C.  20472
Telephone: (202) 384-2874
E-mail: kenneth.vrooman@hq.dhs.gov

**Richard Wyman**
U.S. Department of Energy
Idaho National Laboratory/Batelle Energy Alliance
2525 Fremont Avenue
Idaho Falls, ID  83415
Telephone: (208) 526-1249
E-mail: richard.wyman@inl.gov

**U.S. Environmental Protection Agency**

**Robert Bastian**
U.S. Environmental Protection Agency
Office of Water
Office of Wastewater Management
William Jefferson Clinton Building (4204M)
1200 Pennsylvania Avenue, NW
Washington, D.C.  20460
Telephone: (202) 564-0653
E-mail: bastian.robert@epa.gov

**Steve Clark**
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research Center
William Jefferson Clinton Building (8801R)
1200 Pennsylvania Avenue, NW
Washington, D.C.  20460
Telephone: (202) 564-3784
E-mail: clark.stephen@epa.gov

**Hiba Ernst**
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research Center
Water Infrastructure Protection Division
26 W Martin Luther King Drive (NG-16)
Cincinnati, OH  45268
Telephone: (513) 569-7943
E-mail: ersnt.hiba@epa.gov

**James Goodrich**
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research Center
Water Infrastructure Protection Division
26 W Martin Luther King Drive (NG-16)
Cincinnati, OH  45268
Telephone: (513) 569-7605
Email: goodrich.james@epa.gov

**Eric Koglin**
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research Center
944 E Harmon Avenue
Las Vegas, NV  89119
Telephone: (702) 798-2332
E-mail: koglin.eric@epa.gov

**Jon Richardson**
U.S. Environmental Protection Agency
Office of Research and Development
Office of Science and Information Management
P.O. Box 93478
Las Vegas, NV  89193
Telephone: (702) 798-2601
E-mail: richardson.jon@epa.gov

**Gregory Sayles**
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research Center
26 W Martin Luther King Drive (NG-16)
Cincinnati, OH  45268
Telephone: (513) 569-7607
E-mail: sayles.gregory@epa.gov

**Daniel Schmelling***
U.S. Environmental Protection Agency
Office of Water
William Jefferson Clinton Building (4608T)
1200 Pennsylvania Avenue, NW
Washington, D.C.  20460
Telephone: (202) 564-5281
E-mail: schmelling.dan@epa.gov

**Emily Snyder***
U.S. Environmental Protection Agency
Office of Research and Development
National Homeland Security Research
Center
109 TW Alexander Drive (D143-01)
Research Triangle Park, NC  27709
Telephone: (919) 541-1006
E-mail: snyder.emily@epa.gov

*Participated by teleconference

# APPENDIX B

## Workshop Agenda

**U.S. Environmental Protection Agency (EPA)**
**Subject Matter Expert Meeting to Identify Cybersecurity Research Gaps and Needs of the Nation's Water Sector**

**Ronald Reagan Building and International Trade Center**
**The Policyeum (Conference Room 51161)**
**1300 Pennsylvania Avenue, NW**
**Washington, D.C.**

**March 30 – 31, 2016**

**Agenda**

---

<u>**Wednesday, March 30, 2016**</u>

**8:30 – 8:40 a.m.** **Welcome and Introduction of Participants**
*Gregory Sayles, Acting Center Director, National Homeland Security Research Center, Office of Research and Development (ORD), EPA*

**8:40 – 9:00 a.m.** **Overview of the Workshop**
*Eric Koglin, National Homeland Security Research Center, ORD, EPA*

**9:00 – 9:15 a.m.** **Critical Infrastructure Partnership Advisory Council (CIPAC) Water Sector Cybersecurity Strategy Workgroup Overview**
*Debbie Newberry, Water Security Division, Office of Water, EPA*

**9:15 – 10:15 a.m.** **Water Utility Perspectives**
*Shannon Spence, Arcadis*
*Ed Hackney, United Water, Inc.—SUEZ ENVIRONNEMENT*

**10:15 – 10:45 a.m.** **Break**

**10:45 a.m. – 12:45 p.m.Session One: Cyber Risk Assessment**

1. How can we describe the current and future cyber risks facing the water sector?
2. Considering these risks, how do we best inform decision making in the water sector for—
   a. The range of communications being currently used (e.g., Internet, telephone wires, low-voltage lines, dedicated lines versus the public network, microwaves, cellular, radio waves)?
   b. The capacity differences among small (1,000 to 10,000 people), medium (10,000 to 99,000 people) and large to very large (more than 100,000 people) systems?

As we discuss these areas, please make note of the potential for research and development versus operational needs.

**12:45 – 1:45 p.m.** **Lunch**

**2:00 – 3:00 p.m.** **Department of Homeland Security's (DHS) Industrial Control Systems-Computer Emergency Response Team (ICS-CERT): Threat Experience**
*Bob Timpany, Chief of Operations, ICS-CERT, DHS*

**3:00 – 3:15 p.m.** **Summary of Session One**
*Steve Clark, National Homeland Security Research Center, ORD, EPA*

**3:15 – 3:30 p.m.** **Break**

**3:30 – 5:15 p.m.** **Session Two: Cyber Risk Management**

1. Are there cybersecurity tools developed for other sectors (e.g., electrical power grid, oil/gas pipelines) that could be adapted for use by the water sector?
2. What are the emerging technologies that could be applied to the water sector's risks? Are there vendors solely focused on the water sector's needs?

As we discuss these areas, please make note of the potential for research and development versus operational needs.

**5:15 – 5:30 p.m.** **Summary of Session Two**
*Eric Koglin*

**5:30 p.m.** **Recess**

**Thursday, March 31, 2016**

**8:30 – 9:00 a.m.** **Recap of Day One**
*Steve Clark*

**9:00 – 10:30 a.m.** **Subject Matter Expert Roundtable for Additional Input Into Research and Development Gaps**

**10:30 – 11:00 a.m.** **Break**

**11:00 a.m. – 12:30 p.m.** **Discussion**

Goals: 1. Divide identified research and development needs into the desired defensive elements framework of the *Federal Cybersecurity Research and Development Strategic Plan*
2. Examine short-, mid- and long-term needs, as well as needs by system size.

**12:30 – 1:00 p.m.** **Next Steps and Wrap Up**
*James Goodrich, Senior Science Advisor, National Homeland Security Research Center, ORD, EPA*

**1:00 p.m.** **Adjournment**

# APPENDIX C

## Pre-Meeting List of Recommendations from the Subject Matter Experts

| ***Affiliation*** | ***Stakeholder Group*** | ***Need*** |
|---|---|---|
| SME1 | Industry | Information to help utility management allocate sufficient resources. important cybersecurity programs |
| SME2 | Industry | More is needed to educate/train water utilities on threats and best practices to improve the understanding of vulnerabilities and what can be accomplished through a cyber-attack. |
| SME2 | Industry | The NIST CS Framework and AWWA CS Guidance and Tool are good resources for utilities; SMEs reported that the number of utilities actually applying these is very low. More is needed to get utilities to actually use these. |
| SME3 | Industry | Can we share case studies with other utilities that have embarked on cyber programs: the hows and whys to learn from? |
| SME3 | Industry | Is there information on types of staff a small/medium utility should hire for a general cybersecurity person? What should be on their resume? What is important if a utility can hire only one person or needs to share staff? |
| SME3 | Industry | Guidance for reclassification of labor positions and compensation packages to attract professionals with cybersecurity experience to industry (SCADA, ICS). |
| SME3 | Industry | Research potential benefits and challenges of developing an organization similar to NERC/FERC (power industry) for the water sector. |
| SME4 | Utility | Develop good practice recommendations for using Secure Authentication features; Develop suggestions for distributing and maintaining keys for Secure Authentication; and Encourage adoption of Secure Authentication features among water utilities. |
| SME5 | Utility | Firewall, VPN and IPS/IDS requirements/standards for anyone wanting to connect any ICS/SCADA system to the Internet. |
| SME5 | Utility | Just like EPA has water testing parameters and the AWWA has water meter testing parameters, why not establish cyber testing standards (i.e., adopt an existing standard, but make it apply to the water/wastewater space)? |
| SME6 | Utility | Research the needs for a SCADA Operator Cyber Security Awareness and Training test to see how aware and knowledgeable the SCADA operators and technicians are about the threats and vulnerabilities that face them. |
| SME6 | Utility | Research the possibility for a SCADA Compliance program similar to that of the PCI Compliance program for the payment card industry. This program could spell out the security requirements and require an annual audit. |
| SME7 | Utility | Secure Communications: Identify all the unique issues with protecting DSL, open wireless, DDS, MPLS, Frame Relay, cable network communications, etc. How secure are the Telecom private networks? |
| SME7 | Utility | Secure Communications: Is there an inexpensive approach to effective two-factor authentication for Internet-exposed (remote access) systems? |

| *Affiliation* | *Stakeholder Group* | *Need* |
|---|---|---|
| SME7 | Utility | Secure Communications: What vulnerabilities, besides denial of service, do low-cost Telecom services (e.g., Verizon’s private LTE/EVDO wireless data services) have? |
| SME7 | Utility | Secure Communications: Which data radios, unlicensed and licensed, have properly implemented data encryption? |
| SME2 | Industry | Utilities would benefit by being more explicitly informed that they should do x, y and z to protect their systems. Most utilities may lack even the most basic cybersecurity controls; this is more the case with medium and small utilities, but also applies to large ones. Many issues can be addressed at relatively low cost (e.g., password controls, Internet connectivity, and remote access). |
| SME3 | Industry | Guidance and recommendations on how utilities can organize themselves to bridge gaps between their IT groups and their Operations Groups, where most SCADA/ICS live, to address organizational vulnerabilities. |
| SME3 | Industry | Knowledge of what the prevalent technologies are in the water sector (e.g., Rockwell, Siemans, etc.) to direct efforts. |
| SME3 | Industry | Utilities would like to know specific vulnerabilities of the hardware they own (i.e., Rockwell, Foxboro and Bristol). |
| SME2 | Industry | Vulnerabilities would be reduced significantly if there were a specific set of minimum standards that water utilities had to adhere by, as found in other industries. |
| SME1 | Industry | Secure and consistent methodology for management of process-control-related documentation. |
| SME1 | Industry | Secure, consistent and vendor-independent methodology for mobile access to real-time process control information. |
| SME5 | Utility | What is the responsibility of the System Integrator? Small water/wastewater systems that do not have any IT skills rely heavily on System Integrators. . How can integrators be held responsible for bad designs and careless implementations (i.e., a System Integrator leaves back door remote access to a small system so he or she can easily support it from far away). |
| SME6 | Utility | Research on how we can implement a system for SCADA that is similar to other business applications; one that is modular and allows for Operating Systems (OS) and applications to be upgraded independently from new hardware. One reason the life expectancy of SCADA systems is 10 years or more is because they are “black-box” proprietary systems and are “fork-lift” in nature, requiring a complete system change, which takes years to implement. |
| SME6 | Utility | Research the impacts of an Electro Magnetic Pulse (EMP) attack on a SCADA system, particularly one that is largely spread out over a large service area. Little research is available about the risk and impacts to the computer systems that could be destroyed by an EMP attack. Many SCADA systems are large, geographically dispersed systems. |
| SME7 | Utility | ICS Security Device Review: Are there real practical advantages of preconfigured industrial firewalls like the Hirschmann Eagle? Are they difficult or expensive for smaller water systems to keep patched? |
| SME7 | Utility | Internal Threats: Is there anything different about how OT internal threats present as compared to IT internal threats? Are there any precautions that can be taken? |

| ***Affiliation*** | ***Stakeholder Group*** | ***Need*** |
|---|---|---|
| SME7 | Utility | Lower Profile: Are there simple ways to change Internet-facing equipment service banners so that they appear to be something other than SCADA devices to scans from Shodan, etc.? |
| SME7 | Utility | Protection From Thumb Drives: Are there configuration settings that protect PCs from thumb drive malware? Are the protections provided by Microsoft's Software Restriction Policy of disallowing running software on all non-C: drives and turning off autorun adequate to keep malware from spreading from a USB thumb drive to a SCADA PC? |
| SME3 | Industry | Investigate whether some sort of certification process for utilities that achieve levels of cybersecurity posture would be helpful in lowering costs of general insurance or bond ratings. Such certifications already exist for more general IT but may be out of reach (or impractical) for utilities. |
| SME3 | Industry | Potential rating system for Operation Technology providers (hardware, software) that rates providers' cybersecurity position relative to multiple factors, including number of known vulnerabilities, average time to patch vulnerabilities, etc. |
| SME5 | Utility | Certification program very much like Cisco's "CCIE" certification. There are water and wastewater plant operator licenses. Why not an EPA certification for people working on critical infrastructure control systems? |
| SME7 | Utility | Data Loss Prevention: When disposing of a hard drive, you wipe or degauss it or both. What is the appropriate way to clean a USB thumb drive or SSD SATA drive to make sure there are no data left on the drive? |
| SME7 | Utility | Leveraging Prior Work: Was the LOGIIC Correlation Project or the Sophia Tool successful enough that their successors should be promoted? Are there more appropriate tools for identifying internal anomalies? |
| SME7 | Utility | Revenue Protection: Review of Smart Meter systems for security vulnerabilities. |
| SME8 | Utility | A tool that will develop an "as deployed" checksum of all firmware and drivers on a PC, server or other network device, which can then be periodically verified against the device "as found." |
| SME8 | Utility | Develop a tool to fingerprint a PC with all open ports, services, registry run keys and settings prior to applying a patch, which can then be re-run after patch applications to indicate any new open ports, running services, changes to registry run keys or other settings. |
| SME8 | Utility | Work with vendors to develop a repository of known good software and firmware with hashes. The "SCADA Whitelist" is an open source project that tried that but does not claim that hash is free from defects. This suggestion would take it a step further, where the items in the repository are verified to be clean or at least all vulnerabilities are documented. |
| SME3 | Industry | Utilities would benefit from knowing what's coming—what sort of technology convergence is happening and what it will mean for their operations and cyber posture. |
| SME5 | Utility | Much focus on the water sector, but what about the wastewater sector? Perform scenario planning for a hack of a wastewater collection system and plant—perhaps a tabletop exercise with wastewater SCADA experts—and then break into a pilot system and test the hypotheticals. |

| Affiliation | Stakeholder Group | Need |
|---|---|---|
| SME5 | Utility | Research how bad things can get—set up a pilot water system and connect it to the Internet with a consumer-grade firewall, have a white hat break into the firewall and take control of the water system, try to break things, try to misrepresent quality data, etc. |
| SME5 | Utility | Most of the attention is on SCADA and Control Systems, but there is a large attack surface in other OTs water and wastewater utilities are adopting. Research and catalog. |
| SME6 | Utility | Research the need and capability for providing better information redundancy so that the SCADA system's data integrity can be assured. Operators need to know that the data they are being provided by the SCADA system to make decisions are accurate and not false. This would be a separate alarm system to notify operators when systems are operating outside of safe limits. |
| SME7 | Utility | Water Manager Advice: Are there tips that water managers should have to help them distinguish operator error from a hacking event so that ICS-CERT or others are not called out unnecessarily? |
| SME8 | Utility | An appliance that can act as a sandbox to unpack, install, inspect and analyze software and firmware, which will be transferred into an isolated ICS network, using "fire-eye-like" technology to artificially speed up time to check for unintended activities like port scans, C&C traffic, etc. |
| SME8 | Utility | Research into cyber-physical vulnerabilities and mitigation techniques: Create a "cyber-physical mitigation guide" that outlines methods and considerations for utilities to identify and mitigate vulnerable processes/equipment in their systems. Guide could have examples of common water/wastewater process equipment and/or systems that would be vulnerable to physical damage from a cyber-attack (think Aurora, water hammer, etc.). Guide could identify a non-network-connected safety system that would prevent damage if the OT-based control system was compromised. |
| Other1 | Federal Agency | Conduct water cybersecurity vulnerabilities assessments at up to five utilities, followed by cyber-physical testing of representative utility equipment at EPA's water security test bed at DOE's Idaho National Laboratory. The proposed vulnerability assessments would extend beyond the current ICS-CERT assessment, which stop at the PLC. These assessments will be conducted to the control systems' end devices.<br>Utilities, water industry trade associations and government policymakers need a better understanding of the operational and physical impacts of a cyber-attack on water and wastewater systems. For example, can an attacker maliciously operate pumps to failure? Break mains? Cause discharge violations? Create long-term production outages? If so, what are the cyber exploits needed to cause these impacts? Are there process design modifications that could mitigate or prevent these impacts? |

| *Affiliation* | *Stakeholder Group* | *Need* |
|---|---|---|
| Other1 | Federal Agency | Water sector utilities are starting to use cloud services for supporting operations (weather forecasting, energy management, water quality tracking, reporting, metering, leak detection, backups, network management, etc.) without having a full understanding of the security implications of deploying these technologies. This is also an important issue for policymakers. For instance, what are the regional and/or national impacts of exploiting cloud services that have access to many different types of water and wastewater control systems located throughout the country? |

# APPENDIX D
# Subject Matter Expert Recommendations for Water Cybersecurity Research Needs (Post-meeting)

1. **Cyber-Physical Impacts and Education of Executives**

   Initiate a project to educate executives and decision makers on risks, consequences and liabilities of cyber events. Work with ICS-CERT and DOE's Idaho National Laboratory to identify a water failure demonstration that could raise awareness.

2. **Education and Training. Educate/train water utilities on threats and best practices**

   There is a general lack of understanding of vulnerabilities and what can be accomplished through a cyber-attack. For example, it often takes actually showing a utility how their systems can be viewed online or how their wireless signals can be intercepted before they begin to understand the threats that they face. There is some concern about revealing to too broad an audience on specific vulnerabilities, but this risk can be mitigated and should be considered relative to the risk of not providing this training, as many adversaries are already aware of these vulnerabilities**.**

3. **Training Options**

   Compile a list of existing cybersecurity training options, both free and paid. Identify gaps that relate to water and ways to encourage participation by water and wastewater utility staff.

4. **Cyber-Physical Impacts and Design Mitigations**

   Foster a better understanding of the operational and physical impacts of a cyber-attack on water and wastewater systems among utilities, water industry trade associations and government policymakers. For example, can an attacker maliciously operate pumps to failure, break mains, cause discharge violations, or create long-term production outages? If so, what are the cyber exploits needed to cause these impacts? Are there process design modifications that could mitigate or prevent these impacts?

5. **Cyber-Physical Impacts and Safety System Mitigations**

   Conduct research on cyber-physical vulnerabilities and mitigation techniques. Create a "cyber-physical mitigation guide" that outlines methods and considerations for utilities to identify and mitigate vulnerable processes/equipment in their systems. The guide could have examples of common water/wastewater process equipment and/or systems that would be vulnerable to physical damage from a cyber-attack (think Aurora, water hammer, etc.). The guide could identify a non-network-connected safety system that would prevent damage if the operations technology-based control system was compromised.

6. **Patching Security**

   An appliance that can act as a sandbox to unpack, install, inspect and analyze software and firmware, which will be transferred into an isolated ICS network, using “fire-eye-like” technology to artificially speed up time to check for unintended activities like port scans, command and control traffic, etc.

7. **Vulnerability and Impact Assessments**

   Conduct water and wastewater cybersecurity vulnerability/impact assessments at up to five utilities, followed by cyber-physical testing of representative utility equipment at EPA’s water security test bed at DOE’s Idaho National Laboratory. The cyber-physical tests would identify potential water utility cybersecurity intrusions and physical impacts and raise awareness about these intrusions/impacts. Other potential outcomes could be the identification of existing “best practices” to thwart these intrusions and the development of a water cybersecurity mitigation guide. The proposed vulnerability assessments would extend beyond the current ICS-CERT assessments, which do not go beyond PLCs. These assessments will be conducted to the control systems’ end devices.

8. **Patching Security**

   A tool that will develop an “as deployed” checksum of all firmware and drivers on a personal computer, server, or other network device, which can then be periodically verified against the device “as found.”

9. **Patching Security**

   Develop a tool to fingerprint a personal computer with all open ports, services, registry run keys and settings prior to applying a patch, which can then be re-run after patch applications to indicate any new open ports, running services, or changes to registry run keys or other settings.

10. **Internet-Facing Addresses**

    Initiate a joint campaign by EPA, WaterISAC, AWWA and other sector organizations to encourage water utilities to identify their Internet-facing addresses and test them. Municipal systems could sign up for free monthly scanning by the Multi-State Information Sharing & Analysis Center (MS-ISAC). Private utilities could sign up for free scanning by NCATS. A guide could be created to assist utilities with identifying vendor connections, “black box” cellular connections (e.g., connections to building heating, ventilation, and air conditioning (HVAC) systems), and dial-up access points.

11. **Patching Security**

    Work with vendors to develop a repository of known good software and firmware with hashes. The “SCADA Whitelist” is an open-source project that tried that but does not claim that hash is free from defects. This suggestion would take it a step further, where the items in the repository are verified to be clean or at least having all vulnerabilities documented.

**12. Cloud Services**

Water sector utilities are starting to use cloud services for supporting operations (weather forecasting, energy management, water quality tracking, reporting, metering, leak detection, backups, network management, etc.) without having a full understanding of the security implications of deploying these technologies. This is also an important issue for policymakers. For instance, what are the regional and/or national impacts of exploiting cloud services that have access to many different types of water and wastewater control systems located throughout the country?

**13. Server Hardening**

Develop and test a standardized procedure for configuring servers in a minimum configuration to support process control applications (e.g., eliminate unneeded software, disable unused operating system functions, and disable communication ports).

**14. Security Rating System**

A potential rating system for OT providers (hardware, software) that rates providers' cybersecurity position relative to multiple factors, including number of known vulnerabilities, average time to patch vulnerabilities, etc. A potential rating system for "package panels" that are routinely used in utilities also would be helpful. Further, it would be useful to include wastewater, as well as water utility hardware, in the development of these rating systems.

**15. Documentation Security.**

Secure and consistent methodology for management of process-control-related documentation. Documentation of "best practices" for PCSs are needed.

# Glossary

Human machine interface (HMI): The HMI is the user interface in a manufacturing or process control system. It provides a graphics-based visualization of an industrial control and monitoring system. An HMI typically resides in an office-based Windows computer that communicates with a specialized computer in the plant such as a programmable logic controller (PLC) or distributed control system (DCS).

Network segmentation: It involves splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security. When a cyber-criminal gains unauthorized access to a network, segmentation can provide effective control to limit further movement across the network.

Process control system (PCS): A PCS is a combination of computer software and hardware used to monitor and control the operating environment of a water or wastewater utility based on the various set-points established by the operator. The phrases industrial control system (ICS) and distributed control system (DCS) are synonymously used.

Programmable logic controller (PLC): A PLC is a specialized computer used to automate control of machines used in industrial processes. For example, a PLC can be used to automate when pumps turn on and off.

Remote terminal unit (RTU): An RTU is a device installed at a remote location that collects data, codes the data into a format that is transmittable and transmits the data back to a central location.

Supervisory control and data acquisition (SCADA) system: A SCADA system is a computer-based system for gathering and analyzing real time data to monitor and control equipment used in PCSs.

EPA
United States
Environmental Protection
Agency

Office of Research and Development (8101R)
Washington, DC 20460