Cybersecurity Tools to Understand, Evaluate, and Mitigate Risks

FOR MAINE PUBLIC WATER SYSTEMS

OCTOBER 2019

Assembled by Maine Rural Water Association
with funding from the
Maine Drinking Water Program
Drinking Water State Revolving Fund

mrwa
MAINE RURAL WATER ASSOCIATION

Table of Contents

Purpose and How to Best Use this Document

The purpose of this document is to provide guidance for public water system (PWS) managers and operators relative to performing cybersecurity assessments to quantify and mitigate risks against cyber-attacks. The intent is for PWSs to refer to this as a guidance tool to assist them in the assessment of their system's cyber-resiliency.

Maine Rural Water Association (MRWA) collaborated with Unlimited Technology Associates (UTA), the Maine Drinking Water Program (DWP), the Maine Emergency Management Agency (MEMA), and other partners to create these materials to support PWSs with the tools and resources to increase their cyber-resiliency. MRWA reviewed dozens of existing resources and offers this compilation for PWSs to understand, anticipate, and recover from cyber-attacks. No matter the size of your PWS, these materials will help take you from your current state to a place of increased cyber preparedness.

The following resources were compiled to develop this guidance document:

- Environmental Protection Agency (EPA) "Cybersecurity 101 for Water Utilities", July 2012
- EPA's "Incident Action Checklist – Cybersecurity", October 2017
- EPA's "Water Sector Cybersecurity Brief for States"
- New York State Department of Health Water Supply "Vulnerability Assessment-Cybersecurity"
- National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity", April 16, 2018
- The Water Information Sharing and Analysis Center (WaterISAC) "10 Basic Cybersecurity Measurers - Best Practices to Reduce Exploitable Weaknesses and Attacks", June 2015

A full review of the documents listed above will provide additional information, beyond what is offered here. PWS operators are encouraged to learn as much as possible to make their networks more resilient and ensure that their critical systems are safe.

If simply wanting to know more about how to better protect your PWS doesn't spur you to action, then perhaps a new Federal mandate will. The 2018 America's Water Infrastructure Act (AWIA) requires PWSs to perform cybersecurity assessments and develop a cybersecurity plan. The Act requires PWSs serving a population of greater than 3,300 persons to conduct risk and resilience assessments of their systems, inclusive of "electronic, computer, or other automated systems (including the security of such systems)[1]" and update their emergency response plans. In addition, they must submit certifications to the EPA of the completion of the assessments and updates. Systems serving 100,000 people or more must submit initial certifications by March 31, 2020; systems serving 50,000 to 100,000 people, by December 31, 2020; and systems serving between 3,300 and 50,000 people, by June 30, 2021[1]. Emergency response plan certifications are due six months from the date of the risk assessment certification. Follow up risk and resilience assessments and emergency response plan updates are required every five years thereafter, each of which requires subsequent notification to the EPA recertifying the PWS has complied with the mandate. More information on the AWIA risk assessment and emergency response plan requirements can

[1] America's Water Infrastructure Act of 2018, Section 2013 Community Water System Risk and Resilience

be found on EPA's website at https://www.epa.gov/waterresilience/americas-water-infrastructure-act-2018-risk-assessments-and-emergency-response-plans.

Introduction

PWSs are considered prime targets for cyber-related incidents because of their critical role in supporting primary human functions, disease control, and hygiene. If a PWS were attacked and impaired, it would affect the community's ability to function and remain healthy. Cyber-attacks against the critical infrastructure sector, including PWSs, have increased nationwide, including in Maine. In the past three years, at least six different cybersecurity incidents have been reported from Maine PWSs.

While cyber-threats against Maine PWSs are real, there are also basic steps that any PWS can take to better protect their systems.

For the purposes of this document, cybersecurity and information security will be used interchangeably. Cybersecurity can seem overwhelming but there are two ways of organizing security concepts into categories that can make security more manageable; these are the CIA Triad and the NIST Framework.

The CIA Triad

First, understand your security objectives. Generally, the purpose of any cybersecurity investment or action should be to improve:

- Confidentiality (including data privacy);
- Integrity (including validity and authenticity); and
- Availability

Confidentiality means ensuring that only authorized users have access to information. Integrity means that protections are in place to ensure that data is neither intentionally nor unintentionally changed. Availability refers to a system's ability to perform according to its design when authorized users request service.

Much attention is given to confidentiality in security for business and information technology (IT) assets where theft of sensitive data is harmful. Healthcare and finance, for example, are two industries where confidentiality is the most critical objective. PWSs, however, are most concerned with the availability of systems to perform as designed. An attack on a Supervisory Control and Data Acquisition (SCADA) system or other devices in a PWS could have devastating consequences, not only on the facility but on other critical services such as fire protection and healthcare, as well as the health and wellbeing of an entire community. Accordingly, the goals in securing a PWS are different from the security goals of a hospital or bank, even though many of the same practices, tools, and techniques are employed.

The NIST Framework

The NIST Framework was prepared by the National Institute of Standards and Technology (NIST) with extensive private sector input and issued in February 2014. The NIST Framework for Improving Critical Infrastructure Cybersecurity has five categories:

- Identify;
- Protect;
- Detect;
- Respond; and
- Recover

You must identify all your assets (and devices on your network that you didn't know about); protect authorized assets as best as possible; have the ability to detect malfunctions and malicious activities; respond to incidents according to the level of threat each poses; and have procedures in place for recovery in case there is an incident. It is helpful to be mindful of the function served by each security investment.

A Critical Look: Conducting the Cybersecurity Self-Assessment

The questions in the following Cybersecurity Self-Assessment are tailored to help Maine PWS managers and operators identify risks and improve resiliency. We adapted this assessment tool for ease of administration and heightened review and analysis of key systems. References to the standards, guidelines, and practices to promote the protection of critical infrastructure are provided throughout.

If your PWS is not yet cyber-savvy, then now is the time to become acquainted with the risks and the available remedies. Not all of Maine's PWSs have implemented remote logistical controls, but many have and as time continues, more will. PWSs make unique targets because of their critical mission to provide safe water for primary human functions, disease control, and hygiene. As technology develops, so too will our need for protection of our critical assets. Cyber-attacks are happening now, right here in Maine.

The purpose of the self-assessment is to encourage PWSs to review the questions and take an honest look at their system's vulnerabilities. This includes not only a review of the protection around customer billing accounts and personal information, but also a review of how your PWS could be vulnerable to a cyber-attack via the internet or Local Area Network (LAN).

The self-assessment is not an exhaustive list of cyber-issues and if you have a complex cyber infrastructure, consultation with an IT specialist is advised.

Let's Get Started: *Cybersecurity Self-Assessment Directions*

Answer each of the Cybersecurity Self-Assessment questions. If you need more explanation of any of the terms used in the assessment, refer to the Glossary of Terms section in Appendix A.

With the Cybersecurity Self-Assessment in hand, consult the 12 Basic Cybersecurity Measures section. This section provides guidance for understanding and answering the self-assessment questions. It also offers valuable resources and steps necessary to mitigate or reduce your identified cybersecurity vulnerabilities.

To provide a factual and complete answer to the questions, you may need to consult with others, such as your IT department, SCADA or Process Control System (PCS) vendors, or other knowledgeable IT professionals.

Use the Maine Public Water System Cybersecurity Improvement Plan template (page 16) to catalog the vulnerabilities that you revealed, identify qualified staff to address the vulnerabilities, and determine projected completion dates. This template will help you maintain a running list of vulnerabilities and manage their mitigation.

Maine Public Water System Cybersecurity Self-Assessment[2]

Water System Name: _____ PWSID#: _____ Date: _____

Evaluator(s) [Name(s) & Title(s)]: _____

1. Maintain an accurate inventory of control system devices and eliminate any exposure of this equipment to external networks (see page 16 for more information)	**Yes**	**No**	**N/A**	**Comments**
a) Is there an accurate and up-to-date inventory of all critical systems (process control systems (PCS) and business critical systems (BCS))?	☐	☐	☐	
b) Are software applications and platforms identified and inventoried?	☐	☐	☐	
c) Are the personnel or entities responsible for operating and maintaining critical systems identified in the above-mentioned inventory?	☐	☐	☐	
d) Are there updated physical and logical access control and administrative privileges lists of all PWS and non-PWS personnel with access to critical systems?	☐	☐	☐	
e) Are the data flows mapped?	☐	☐	☐	
f) Are the external/cloud-based resources catalogued?	☐	☐	☐	

[2] Adapted from the NY State Department of Health Water Supply Vulnerability Assessment - Cybersecurity and National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*

2. Defining cybersecurity policies & regulatory requirements (see page 16 for more information)	Yes	No	N/A	Comments
a) Have legal and regulatory requirements been considered?	☐	☐	☐	
b) Are organizational information security policies established?	☐	☐	☐	
c) Are information security roles and responsibilities established?	☐	☐	☐	
d) Is there an assigned Cybersecurity Officer?	☐	☐	☐	
e) Are cybersecurity roles and responsibilities of employees identified?	☐	☐	☐	
f) Is there a written Cybersecurity Policy for all staff at the PWS?	☐	☐	☐	
g) Is there a written Cybersecurity Policy for outside entities (e.g. vendors, contractors/service providers, etc.)?	☐	☐	☐	
h) Are mobile devices (e.g. laptops, tablets, smartphones), used to access or control PCS equipment, included in established Cybersecurity Policies?	☐	☐	☐	
i) Is there a company policy addressing employees' uses of personal electronic devices (BYOD) for work purposes?	☐	☐	☐	
j) Are there established BYOD security measures (e.g. policies, contracts) that address uses of personal electronic devices by contractors and independent agents?	☐	☐	☐	
k) Are there written policies for removing or permanently destroying any stored data when removing devices from service for all devices with memory capabilities (e.g. laptops, multi-function printers, cell phones, etc.)?	☐	☐	☐	
3. Evaluating threats & vulnerabilities (see page 17 for more information)	**Yes**	**No**	**N/A**	**Comments**
a) Are cybersecurity self-assessments/audits completed and up to date (e.g. initially and after changes occur)?	☐	☐	☐	
b) Was a vulnerability management plan developed and implemented?	☐	☐	☐	
c) Are vulnerabilities in assets identified and documented?	☐	☐	☐	

d) Are internal threats identified and documented?	☐	☐	☐	
e) Are external threats identified and documented?	☐	☐	☐	
f) Are sources for receiving threat and vulnerability information established?	☐	☐	☐	
g) Do the vulnerability assessments conducted include the risk and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits?	☐	☐	☐	
h) Are periodic vulnerability scans conducted on critical systems and hosted applications for operating system(s), web application(s), and database(s) (as applicable) and when new vulnerabilities potentially affecting the system/applications are identified and reported?	☐	☐	☐	
i) Have independent, third party "penetration tests" been conducted to evaluate the security of all internet facing devices?	☐	☐	☐	
j) Are cybersecurity threat and vulnerability updates from information sharing entities such as US-CERT, WaterISAC, and/or IT vendors/consultants being received?	☐	☐	☐	
4. Establishing a risk management strategy (see page 17 for more information)	**Yes**	**No**	**N/A**	**Comments**
a) Are key functions of "mission critical objectives" identified in the above-mentioned inventory?	☐	☐	☐	
b) Have resilience requirements to support delivery of critical services been established?	☐	☐	☐	
c) Have dependencies and critical functions for delivery of critical services been established?	☐	☐	☐	
d) Are risk management processes established and agreed to by all stakeholders including executive management?	☐	☐	☐	
e) Has the organization's tolerance for risk been determined and clearly expressed?	☐	☐	☐	

f) Does the organization's risk tolerance take into consideration the role played in the community's critical infrastructure?	☐	☐	☐	
g) Have resources been classified based on their criticality?	☐	☐	☐	
h) Has an analysis of risk based on threats, vulnerabilities, likelihoods and impacts been assessed?	☐	☐	☐	
i) Has the impact of each potential threat and the likelihood of occurrence been assessed?	☐	☐	☐	
j) Have the risks and benefits (pros/cons) of completely disconnecting critical systems from all networks been evaluated?	☐	☐	☐	
5. Protections for identity management and access control (see page 18 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Are critical systems physically secured from unauthorized personnel?	☐	☐	☐	
b) Have password policies been put in place to require strong passwords which are changed regularly?	☐	☐	☐	
c) Have password policies been put in place which require each user to have unique credentials to log in to all critical systems?	☐	☐	☐	
d) Have password policies been put in place which require different log in credentials for critical systems?	☐	☐	☐	
e) Have password policies been put in place which require auto screen saver with password protection on all critical systems?	☐	☐	☐	
f) Are administrative privileges used only when carrying out administrative functions on the system?	☐	☐	☐	
g) Are there restrictions (e.g. procedures/polices) on who can/cannot install software and updates?	☐	☐	☐	
h) Are user permissions based on principles of least privilege and separation of duties?	☐	☐	☐	
i) Are critical systems' account privileges restricted to basic access levels to complete desired task(s)?	☐	☐	☐	

j) When personnel are no longer employed (whether terminated or resigned) are their credentials within the systems terminated immediately?	☐	☐	☐	
6. Empowering staff through awareness and training (see page 19 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Are staff at all organizational levels periodically trained on the PWS's cybersecurity policy?	☐	☐	☐	
b) Are all outside entities periodically trained on the PWS's cybersecurity policy?	☐	☐	☐	
c) Are staff at all organizational levels periodically trained on their cybersecurity roles and responsibilities?	☐	☐	☐	
d) Are staff at all organizational levels periodically trained on cybersecurity threats?	☐	☐	☐	
e) Are all essential personnel trained to perform mission critical functions during a cyber incident that disables critical systems (e.g. able to manually monitor and control critical functions)?	☐	☐	☐	
f) Are drills/exercises conducted for responding to cyber incidents that disable critical systems?	☐	☐	☐	
g) Do all personnel understand their roles in the event of an emergency?	☐	☐	☐	
7. Establishing data security protection (see page 19 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Is data at rest protected?	☐	☐	☐	
b) Is encryption used for all data transfers including transfers over wireless links?	☐	☐	☐	
c) Have critical systems that can be disconnected from networks been disconnected?	☐	☐	☐	
d) Are PCS prevented from "talking" directly to BCS on a network or on the internet?	☐	☐	☐	
e) Is remote access via local area network, internet, or other means, protected by firewall, password, dial back protocol, and/or secure tokens?	☐	☐	☐	
f) Have non-PCS functions been blocked on PCS devices, including internet browsing and email access?	☐	☐	☐	

g) Have unnecessary USB, DVD, and other external media ports been disabled?	☐	☐	☐	
h) Have “AutoRun” and “AutoPlay” features of removable media been disabled?	☐	☐	☐	
i) Is remote access managed via an appropriately secure connection?	☐	☐	☐	
j) For devices with memory capabilities (e.g. laptops, multi-function printers, cell phones, etc.) are there written policies in place for transferring devices from one employee to another?	☐	☐	☐	
k) Are mobile devices (e.g. laptops, tablets, smartphones) which are used to access or control PCS equipment encrypted?	☐	☐	☐	
l) Are mobile devices (e.g. laptops, tablets, smartphones), which are used to access or control PCS equipment, dedicated for PCS use only and is non-essential software removed and are unnecessary functions disabled?	☐	☐	☐	
8. Implementing information protection processes and procedures (see page 20 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Are there formal policies for managing removal, transfers and disposal of data?	☐	☐	☐	
b) Are there configuration change policies and processes in place?	☐	☐	☐	
c) Do you perform “due diligence” before hiring a contractor?	☐	☐	☐	
d) Are third-party contractors held liable in the event of a cybersecurity breach for which they are responsible, including subcontractors and supply chain risks?	☐	☐	☐	

e) Do you have internal policies and a contract for third-parties that specifies confidentiality, audits/inspections, security measures, and deletion/return of data and access privileges upon contract termination?	☐	☐	☐	
f) Do third party stakeholders know and understand their roles and responsibilities?	☐	☐	☐	
9. Protecting resources through maintenance (see page 21 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Are periodic repairs and maintenance performed on assets?	☐	☐	☐	
b) Are security patches installed on all critical systems regularly?	☐	☐	☐	
c) Are there mechanisms for verifying data integrity when new software, firmware or processes are employed?	☐	☐	☐	
10. Detect Malware (see page 21 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Do critical systems use anti-virus and anti-malware software?	☐	☐	☐	
b) Are critical systems regularly updated with virus and malware definitions?	☐	☐	☐	
c) Are critical systems storage media regularly scanned for viruses and malware?	☐	☐	☐	
d) Do critical systems use application whitelisting, which allows execution of approved files, applications and programs only?	☐	☐	☐	
11. Ensuring anomalies and events are detected (see page 22 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Is a baseline of network operations and expected data flows (e.g. volume of data flow) for users and systems established?	☐	☐	☐	
b) Are audit logs maintained and reviewed?	☐	☐	☐	
c) Is the physical environment monitored for suspicious activity?	☐	☐	☐	
d) Is the network monitored to detect and alert on potential cybersecurity events?	☐	☐	☐	

e) Are there controls in place to monitor for unauthorized personnel, connections, devices and software?	☐	☐	☐	
f) Are notifications from detection systems consistently investigated?	☐	☐	☐	
12. Ensuring the organization implements recovery planning (see page 22 for more information)	**Yes**	***No**	**N/A**	**Comments**
a) Has a Cybersecurity Emergency Response/Disaster Recovery Plan been established?	☐	☐	☐	
b) Does the Cybersecurity Emergency Response/Disaster Recovery Plan include details for cyber incident reporting to appropriate internal and external officials (e.g. local, County, State and Federal)?	☐	☐	☐	
c) Is the Cybersecurity Emergency Response/Disaster Recovery Plan reviewed, exercised and updated periodically (e.g. at least annually)?	☐	☐	☐	
d) Are system and data backups performed regularly (e.g. nightly data backup, weekly main backup)?	☐	☐	☐	
e) Are backups kept at an offsite, secure location?	☐	☐	☐	
f) Has your ability to successfully restore critical systems with backups been validated?	☐	☐	☐	
g) Is an uninterruptable power supply used for continuous control of critical systems?	☐	☐	☐	
h) Is there a contingency for continuous control of critical systems during long term loss of power events?	☐	☐	☐	

***** Refer to the Maine Public Water System Cybersecurity Improvement Plan on page 15 for any "No" answers. Record identified and/or potential vulnerabilities for further evaluation and corrective actions.

Additional Comments & Notes:

Maine Public Water System Cybersecurity Improvement Plan[3]

Water System Name:_____ **PWSID#:** _____ **Date:** _____

Record all identified vulnerabilities in the below table. Individually per vulnerability, list the corrective actions to remove/reduce the threat, lead individual and supporting individual, priority (high, medium or low) based on the severity and projected corrective action completion date.

Question Number and Corrective Action	Lead Individual	Supporting Individual / Company	Priority (High/ Medium/ Low)	Projected Completion Date

[3] Adapted from the NY State Department of Health Water Supply Vulnerability Assessment - Cybersecurity

12 Basic Cybersecurity Measures[4]

This section is designed to assist with understanding and completing the: Maine Public Water System Cybersecurity Self-Assessment. It offers valuable tips, resources, and steps necessary to mitigate or reduce identified vulnerabilities.

1. **Maintain an Accurate Inventory of Control System Devices and Eliminate Any Exposure of this Equipment to External Networks.**

   Purpose: *Identify physical hardware and software assets within the organization to establish the basis of a cyber-asset management program.*

   Narrative: Keep an inventory of control system devices and eliminate any exposure of this equipment to networks outside the PWS. PWSs may not realize this connection exists, but a persistent cyber threat actor can find pathways and use them to access and exploit process control systems to attempt to create a physical consequence. Therefore, PWSs are encouraged to conduct thorough assessments of their systems to determine where pathways exist. Any channels between devices on the PCS and equipment on other networks should be eliminated to reduce network vulnerabilities.

   Resources:

   - ICS-ALERT-11-343-01A Control System Internet Accessibility (ICS-CERT)
   - ICS-ALERT-12-046-01A Increasing Threat to Industrial Control Systems (ICS-CERT)
   - Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

2. **Defining Cybersecurity Policies & Regulatory Requirements**

   Purpose: *Define cybersecurity policies within the organization as well as identifying legal and regulatory requirements regarding the cybersecurity capabilities of the organization.*

   Narrative: An understanding of the assets held and the data workflows along with related vulnerabilities should be the drivers of the policies PWSs adopt. It's also important to include executives in the policy development process. Despite the ever-increasing number of cyber threats and the far-reaching effects cyber-attacks can have, researchers have found that organizational leaders are often unaware of cybersecurity threats and needs. Involving executives (e.g. trustees, directors) in cybersecurity will help them to address cybersecurity in their interactions with external stakeholders, such as if they are questioned following an incident. Cyber-attack victim organizations realized, "how crucial strong, consistent communication is in the wake of major breaches," given the calls for timely information and the speculation that will arise when it is not provided.

[4] Adaptation of WaterISAC 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weaknesses and Attacks, October 2016

Resources:

- Cybersecurity Questions for CEOs (US-CERT)
- Firewall Deployment for SCADA and Process Control Networks (UK Centre for the Protection of National Infrastructure via ICS-CERT)
- Guide to Industrial Control Systems Security – Special Publication 800-82 (NIST)
- Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICSCERT)
- Why You Need to Segment Your Network for Security (CSO)

3. Evaluating Threats & Vulnerabilities

Purpose: *Evaluate asset vulnerabilities, threats to internal and external organizational resources, and risk response activities as a basis for the organizations risk assessment.*

Narrative: Consider conducting vulnerability assessments (VA) and scanning on your PCSs and BCSs. A VA is a systematic examination to determine the adequacy of security and privacy measures and identify any security and privacy deficiencies. In addition, a VA can provide data from which to predict the effectiveness of proposed security and privacy measures and confirm the adequacy of such measures after implementation.

A VA is an inspection of the security holes that may be exploited on a computer or network. A vulnerability scan detects and classifies system weaknesses in computers, networks, and communications equipment and predicts the effectiveness of countermeasures. A scan may be performed by an organization's IT department or a security service provider.

Resources:

- Assessing Security and Privacy Controls in Federal Information Systems and Organizations - *Building Effective Assessment Plans* (NIST)
- Index of Advisories by Vendor (ICS-CERT)
- Technical Guide to Information Security Testing and Assessment (NIST)

4. Establishing a Risk Management Strategy

Purpose: *Establish a risk management strategy for the organization including establishing risk tolerances.*

Narrative: The threats to information systems include equipment failure, environmental disruptions, human or machine errors, and purposeful attacks that are often sophisticated, disciplined, well-organized, and well-funded. When successful, attacks on information systems can result in serious or catastrophic damage to organizational operations and assets, individuals, other organizations, and the Nation. Therefore, it is imperative that organizations remain vigilant and that senior executives, leaders, and managers throughout the organization understand their responsibilities and are accountable for protecting organizational assets and for managing risk.

Resource:

- The Risk Management Framework (NIST)

5. Protections for Identity Management and Access Control

Purpose: *Utilize protections for identity management and access control within the organization including physical and remote access.*

Narrative: Use strong passwords to keep your systems and information secure and have different passwords for different accounts. Hackers can use readily available software tools to try millions of character combinations to attempt an unauthorized login – this is called a "brute force attack." Passwords should have at least eight characters, but longer passwords are stronger. Include uppercase and lowercase letters, numerals, and special characters. Change all default passwords upon installation of new software, particularly for administrator accounts and control system devices, and regularly thereafter. Implement other password security features, such as an account lock-out that activates when too many incorrect passwords have been entered. Organizations may also consider requiring multi-factor authentication, which entails users verifying their identities – via codes sent to devices they previously registered – whenever they attempt to sign-in.

Role-based access controls are also important to limit the ability of individual users – or attackers – to reach files or parts of the system they shouldn't access. For example, SCADA system operators likely do not need access to the billing department or certain administrative files. Therefore, define the permissions based on the level of access each job function needs to perform its duties, and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. Role-based access controls can facilitate tracking network intrusions or suspicious activities during an audit.

The ability to remotely connect to a network has added a great deal of convenience for end users, but a secure access method, such as a Virtual Private Network (VPN), should be used if remote access is required. A VPN is an encrypted data channel for securely sending and receiving data via public IT infrastructure (such as the internet). Through a VPN, users can remotely access internal resources like files, printers, databases, or websites as if directly connected to the network. This remote access can further be hardened by reducing the number of Internet Protocol (IP) addresses that can access it by utilizing network devices and/or firewalls to specific IP addresses and/or ranges and from within the United States. Note that a VPN is only as secure as the devices connected to it. A laptop computer infected with malware can introduce those vulnerabilities into the network, leading to additional infections and negating the security of the VPN.

Resources:

- Configuring and Managing Remote Access for Industrial Control Systems (ICS-CERT)
- Virtual Private Networking: An Overview (Microsoft)
- An Introduction to Role Based Access Control (NIST)
- Extending Role Based Access Control (SANS Institute)
- Choosing and Protecting Passwords (US-CERT)
- Supplementing Passwords (US-CERT)
- Strong Passwords (Microsoft)

6. Empowering Staff Through Awareness and Training

Purpose: *Empower staff within the organization through awareness and training including role based and privileged user training.*

Narrative: Like any security enterprise, cybersecurity requires teamwork with all members of the PWS playing a part in identifying potential threats and vulnerabilities and bringing them to the attention of others. When employees aren't involved in cybersecurity, not only can vulnerabilities and threats go unnoticed, but the employees themselves can become conduits through which attacks are executed. Therefore, employees should receive initial and periodic cybersecurity training, helping to maintain the security of the PWS as a whole.

While cybersecurity is an expansive field, there are certain topics that should be emphasized for general awareness. One such topic is social engineering, which continues to be a popular means for cyber criminals to prey upon unsuspecting employees. These methods involve emails ("phishing"), phone calls, or other types of personal interactions in which malicious actors attempt to entice employees into providing sensitive personal or corporate information, such as account passwords or details about information technology infrastructure. Alternatively, these actors might attempt to make employees perform specific actions, such as pay for alleged services, download infected attachments, or visit malicious websites. Unsolicited emails, phone calls, and other correspondence from unknown senders should be viewed with caution.

Training should also incorporate the importance of smart internet browsing practices. Visiting suspicious websites may expose users to infection by malware embedded on the site (a "drive-by-download" attack). Even legitimate websites, as well as the files on them, may be compromised. Cyber-attackers employ a variation of this type of tactic, a "watering-hole" attack, to target the employees of a company they know will visit the website. Therefore, caution should be exercised no matter where a user navigates and the materials that are downloaded.

Resources:

- Avoiding Social Engineering and Phishing Attacks (US-CERT)
- Recognizing and Avoiding Email Scams (US-CERT)
- Securing Your Web Browser (US-CERT)

7. Establishing Data Security Protection

Purpose: *Establish data security protection consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.*

Narrative: Never allow a process control system (PCS) to talk directly to a machine on the business-critical system (BCS) or on the internet. Although some PWSs' PCS may not directly face the internet, a connection still exists if those systems are connected to a part of the network that has a communications channel to external (non-trusted) resources (e.g. to the internet).

Network segmentation entails classifying and categorizing IT assets, data, and personnel into specific groups, and then restricting access to these groups. By placing resources into different areas of a network, a compromise of one device or sector cannot translate into the exploitation of the entire system. Otherwise, cyber threat actors would be able to exploit any vulnerability within a PWS – the "weakest link in the chain" – to gain entry and move laterally throughout

a network and access sensitive equipment and data. Given the rise of the "Internet of Things" – whereby many previously non-internet connected devices, such as video cameras, are now linked to systems and the web – the importance of segmenting networks is greater than ever.

Access to network areas can be restricted by isolating them entirely from one another, which is optimal in the case of PCS (as described in recommendation #1 above), or by implementing firewalls. A firewall is a software program or hardware device that filters the inbound and outbound traffic between various parts of a network or between a network and the internet. For connections that face the internet, a firewall can be set up to filter incoming and outgoing information. By reducing the number of pathways into and within your networks and by implementing security protocols on the pathways that do exist, it is much more difficult for a threat to enter your system and gain access to other areas.

Creating network boundaries and segments empowers a PWS to enforce both detective and protective controls within its infrastructure. The capability to monitor, restrict, and govern communication flows yields to a practical capability to baseline network traffic (especially traffic traversing a network boundary), and identify anomalous or suspicious communication flows.

These boundaries also provide a means to practically detect potential lateral movement, network foot printing and enumeration, and device communications attempting to traverse from one zone to another.

Resources:

- Beginners Guide to Firewalls: A Non-Technical Guide (MS-ISAC)
- Firewall Deployment for SCADA and Process Control Networks (UK Centre for the Protection of National Infrastructure via ICS-CERT)
- Guide to Industrial Control Systems Security – Special Publication 800-82 (NIST)
- Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies (ICSCERT)
- Why You Need to Segment Your Network for Security (CSO)

8. Implementing Information Protection Processes and Procedures

Purpose: *Implement information protection processes and procedures to maintain and manage the protections of information systems and assets.*

Narrative: The proliferation of laptops, tablets, smartphones, and other mobile devices in the workplace presents significant security challenges. The mobile nature of these devices means they are potentially exposed to external, compromised applications and networks and malicious actors. Further contributing to this challenge is the increasing trend of organizations allowing employees to use their personal electronic devices for work purposes, known as the "Bring Your Own Device (BYOD)" phenomenon.

Therefore, it's important to develop policies on the reasonable limits of mobile devices in your office and on your networks. These measures should be strictly enforced for all employees, as well as for contractors. Devices should also be password protected to ensure only authorized users can log-in. Otherwise, an unauthorized user can gain access to restricted networks and files using an authorized user's device. Similarly, employees should avoid or be cautious about using devices that do not belong to them as they cannot be sure these are properly protected or

comply with established policy. Such devices may be infected and using them could put the information and networks you access at risk.

Resources:

- Bring Your Own Device (BYOD) Design Considerations Guide (Microsoft)
- Cybersecurity for Electronic Devices (US-CERT)
- Guidelines on Cell Phone and PDA Security (NIST)

9. **Protecting Resources Through Maintenance**

Purpose: *Protect organizational resources through maintenance, including remote maintenance.*

Narrative: Most vendors work diligently to develop patches for identified vulnerabilities. But even after patches and updates have been released, many systems remain vulnerable because PWSs are either unaware of or choose to not implement these fixes. These unpatched vulnerabilities amount to a "low-hanging fruit" for which cyber criminals can easily take advantage.

To protect one's PWS from these opportunistic attacks, a system of monitoring for and applying system patches and updates should be implemented. WaterISAC regularly posts information on vulnerabilities and patches, which it receives from its partners at the U.S. Department of Homeland Security's ICS-CERT and United States Computer Emergency Readiness Team (US-CERT), other ISACs, cybersecurity firms and others. When possible, organizations should consider setting systems and software to auto-update to avoid missing critical updates. These updates are designed to fix known vulnerabilities and are encouraged for any internet connected device.

Resource:

- Recommended Practice for Patch Management of Control Systems (ICS-CERT)

10. **Detect Malware**

Purpose: *Detect and prevent unauthorized software from executing by deploying antivirus technology and application whitelisting.*

Narrative: Computer viruses continue to pose a threat to the integrity and availability of computer systems. This is especially true for users of personal computers. A variety of anti-virus tools are now available to help manage this threat. These tools use a wide range of techniques to detect, identify, and remove viruses.

Resources:

- A Guide to the Selection of Anti-Virus Tools and Techniques (NIST)
- Malware Threats and Mitigation Strategies (US-CERT)

11. Ensuring Anomalies and Events Are Detected

Purpose: *Ensure anomalies and events are detected, and their potential impact is understood.*

Narrative: Implementing a logging capability allows for the monitoring of system activity. This enables organizations to conduct thorough root cause analyses to find the sources of issues in the system, which may have been the activities of an employee or an outsider. Monitoring network traffic also allows organizations to determine if a user is making unauthorized actions or if an outsider is in the system, which provides an opportunity to intervene before problems are manifested.

Measures such as implementing intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), anti-virus software, and logs can help to detect compromises in their earliest stages. Most IDSs and IPSs use signatures to detect port scans, malware, and other abnormal network communications. New viruses are discovered every day, and anti-virus programs are oftentimes set to automatically update themselves to look for the latest threat signatures. Still, administrators should not rely solely on anti-virus software for detecting infections. Logs from firewalls, intrusion detection and prevention sensors, and servers should be monitored for signs of infections.

Resources:

- Alerts, Reports, Best Practices and More (WaterISAC)
- Targeted Cyber Intrusion Detection and Mitigation Strategies (ICS-CERT)

12. Ensuring the Organization Implements Recovery Planning

Purpose: *Ensure the organization implements recovery planning processes and procedures to restore systems and/or assets affected by cybersecurity incidents.*

Narrative: Despite the many preventative measures PWSs implement, many still experience compromises. Indeed, many cybersecurity experts have noted that experiencing a compromise is not really a question of "if," but more of a question of "when." When a compromise occurs, the organizations that fare the best will be those that quickly detect the issue and have a plan in place to respond.

Incident response plans are a critical yet underutilized component of emergency preparedness and resilience. An effective cybersecurity emergency response/disaster recovery plan will limit damage, increase the confidence of partners and customers, and reduce recovery time and costs. Plans should include measures for reacting to destructive malware in a PCS environment. In such situations, organizations should be prepared to "island" their PCS environments by disconnecting from non-PCS networks.

They should also go to "manual operations" if network conditions impact visibility from the SCADA system, or if malware potentially renders control devices inoperable via automated means. In addition, the plan should include a list of critical IT vendors and their regular and after hours contact information.

Rather than being developed by a single entity, the plan should be a product of collaboration between all departments that would-be stakeholders in a cybersecurity incident. This will ensure a cooperative and unified response that leverages all an organization's resources to the greatest extent possible. For enhanced responsive capability in the event of a cybersecurity

incident, organizations should consider forming a Computer Security Incident Response Team (CSIRT).

This task is not complete once the plan has been developed; it needs to be operationalized as well. It is critical that plans be routinely reviewed and updated to ensure they remain relevant and useable for when they are needed. Furthermore, to truly understand their cybersecurity incident response plan, organizations must practice them through regular exercises. This will ensure that all stakeholders understand the procedures that would be implemented in the event of a significant cyber disruption or breach, enabling a more effective and efficient response.

Resources:

- Best Practices for Continuity of Operations (ICS-CERT)
- Create a CSIRT (CERT)
- Cyber Incident Reporting: *A Unified Message for Reporting to the Federal Government* (DHS)
- Developing an ICS Cybersecurity Incident Response Capability (ICS-CERT)
- Drinking Water System Risk Assessments and Emergency Response Plans Required Under America's Water Infrastructure Act (AWIA) (WaterISAC)
- EPA's Incident Action Checklist – Cybersecurity (USEPA)
- Resources for Security and Emergency Response Planning (Maine Drinking Water Program)
- Ten Steps to Planning an Effective Cyber-Incident Response (Harvard Business Review)
- Water Sector Cybersecurity Brief for States (USEPA)

Cyber Incident Action Planning

Now that you've assessed your critical systems, identified vulnerabilities and developed your cybersecurity improvement plan, it's time to develop a cyber incident action plan. As detailed in the 12 Basic Cybersecurity Measures, subsection 12, "Ensuring the Organization Implements Recovery Planning," having an effective cyber incident response plan is a critical component of a PWS's emergency preparedness and resilience. Your PWS's plan should include measures to:

- Detect and respond to a cyber incident/attack,
- Promptly and effectively assess the situation and scope,
- Notify key PWS personnel, local law enforcement, primacy agencies and others,
- Activate and coordinate response activities, including establishing an incident command center,
- Develop a communication plan and designate a Public Information Officer, and
- Implement critical systems recovery once the cyber incident has been eradicated/isolated.

The EPA's Incident Action Checklist - Cybersecurity[5] is a useful reference for developing your PWS's plan to prepare for, respond to and recover from cyber incidents and attacks.

Once your cyber incident action plan has been developed, you may consider incorporating it with your PWS's all hazards emergency response plan or maintain it as a stand-alone plan. In either case, your appropriate PWS personnel should fully understand the plan and their roles and

[5] EPA Incident Action Checklist – Cybersecurity, 2017

responsibility during a cyber incident. In addition, your cyber incident action plan should be reviewed, exercised and updated at least annually. It should also be reviewed and updated as needed after a cyber incident.

To further assist you with developing your cyber incident action plan and a "rip and run" of your plan, the Maine Public Water System Cyber Incident Action Plan offers a basic checklist of the initial response actions to take upon discovery of a cyber incident. In addition, it lists some of the entities that should be notified and provides room to add your own.

Maine Public Water System Cyber Incident Action Plan[6]

Action Checklist

- ☐ Disconnect compromised IT/critical systems from the network. Do *not* turn off or reboot systems.
- ☐ Assess the scope of the compromise and isolate all affected IT/critical systems.
- ☐ Open a ticket with your antivirus software or security service vendor.
- ☐ Assess any potential damage, including impacts to treatment processes or service disruptions.
- ☐ Initiate manual operation of equipment if control systems have been compromised.
- ☐ Distribute any advisories or alerts to customers as needed, including customers whose records may have been compromised.
- ☐ Identify methods to scan all IT/critical systems to eradicate malicious code. Assess and implement recovery procedures.

Reporting Checklist

- ☐ Report the incident to local law enforcement, primacy agencies and others:
  - Maine Drinking Water Program (DWP) – *Maine Public Water Systems*
  - Maine Public Utilities Commission (PUC) – *PUC Regulated Utilities*
  - Maine Emergency Management Agency (MEMA)
  - County Emergency Management
  - Maine Information and Analysis Center (MIAC)
  - Federal Bureau of Investigation (FBI) – Local Office
  - Maine Water/Wastewater Agency Response Network (MEWARN)
- ☐ Contact the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCIC@hq.dhs.gov. NCCIC can assist your PWS with identifying and restoring affected systems
- ☐ Submit an incident report through WaterISAC (analyst@waterisac.org; 866-H2O-ISAC).

[6] Adapted from EPA Water Sector Cybersecurity Brief for States

Important Contact Information

Company/Agency	Point of Contact	Phone Number	Email/Website
IT Service Vendor			
Local Law Enforcement			
Maine Information and Analysis Center		877-786-3636	www.maine.gov/miac/about/miac_contactus.html (online report form)
Maine Drinking Water Program (DWP)	Assigned Public Water System (PWS) Inspector	Phone # of your PWS Inspector: _____ DWP phone #: 207-287-2070 DWP after-hours phone #: 207-557-4214	
Maine Emergency Management Agency		207-624-4400 207-851-8898: After-hours pager	
County Emergency Management Agency	County EMA Director		www.maine.gov/mema/ema-community/county-local/county-emergency-management-agencies (website list of County EMAs)
Maine Public Utilities Commission		207-287-3831	
FBI – Boston, MA Office		857-386-2000	boston.fbi.gov (website)
MEWARN	Maine Rural Water Association	207-737-4092	www.mewarn.org (website)
NCCIC		888-282-0870	NCCIC@hq.dhs.gov
WaterISAC		866-426-4722	analyst@waterisac.org

Appendix A - Glossary of Terms

Access Control: The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities.

Anti-malware: A program designed to protect computers and networks against any threats or attacks from viruses such as adware, spyware, and other malicious programs.

Anti-virus: A program or a set of programs that help prevent malicious objects, codes, and programs from entering your computer or network. If malicious programs enter your computer, antivirus software helps detect, quarantine, or remove such programs from the computer or networks.

AutoPlay & AutoRun: A feature in personal computers that runs a program on a CD/DVD or USB drive. AutoRun is considered a security risk because a virus could be unleashed when the medium is inserted. AutoPlay is the Windows dialog box that appears when an external medium is inserted, offering the user options to play, run or view the content.

Business Critical System (BCS): A general term that includes several types of processes and devices that enable PWS business functions including payroll, accounts receivable/accounts payable, PWS bank accounts, etc. The BCS consists of combinations of in-house and online interfaces and platforms.

Bring Your Own Device (BYOD): BYOD refers to the policy of permitting employees to bring personally owned devices (e.g. laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

Critical systems: A general term used to describe business critical systems (BCS) and/or process control systems (PCS).

Cybersecurity: Cybersecurity includes the processes employed to safeguard and secure assets used to carry information of an organization from being stolen or attacked. It requires extensive knowledge of the possible threats, such as virus or such other malicious objects. Identity management, risk management and incident management form the crux of the cybersecurity strategies of an organization.

Data Flow: A general term that indicates the movement of data through a system comprised of software, hardware or a combination of both.

Dial Back Protocol: The use of dial-up lines as a backup to dedicated lines.

Due Diligence: The investigation or exercise of care that a reasonable person is expected to take before entering into an agreement or contract with another party, or an act with a certain standard of care.

Encryption: A process of maintaining data integrity and confidentiality by converting plain data into a secret code with the help of an algorithm. Only authorized users with a key can access encrypted data or cipher text.

Exploit: A piece of software, a chunk of data, or a sequence of commands that takes advantage of a vulnerability to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic.

Firewall: A security system, tool that includes any software or hardware aimed at preventing viruses, worms, and hackers from intruding into a system or network.

Industrial Control Systems (ICS): See process control systems (PCS).

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Local Area Network: A local area network (LAN) is a computer network that links devices within a building or group of adjacent buildings.

Log In Credential: The process by which an individual gains access to a computer system by identifying and authenticating themselves. The user "log in credentials" are typically some form of username and a matching password and these credentials themselves are sometimes referred to as a log in system by identifying and authenticating themselves.

Malware: A short term used for malicious software. Malware is defined as any software that is used to interrupt or disrupt computer operations, gather sensitive information, or gain access to certain files or programs.

Mission Critical Functions: Mission critical functions are specific functions that are performed to achieve "mission critical objectives" as defined by the PWS. Example #1: PCS controls a water pump (the mission critical function) to maintain a defined water level in a storage reservoir to continuously maintain no less than 20 pounds per square inch (psi) in the entire water distribution system (the mission critical objective). Example #2: BCS processes water usage data (the mission critical function) to process accurate customer bills on a quarterly schedule (the mission critical objective).

Mission Critical Objectives: Mission critical objectives are objectives that are essential to the operation of the PWS. If a mission critical objective is not achieved, it could significantly impact the PWS's ability to provide safe, reliable water for drinking and/or fire protection. In addition, mission critical objectives are associated with both critical process control functions (e.g. water pumping and treatment) and critical business control functions (e.g. customer billing and recordkeeping).

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Penetration Test: Also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities.

Process Control Systems (PCS): Also known as industrial control systems (ICS). A general term that includes several types of control systems, including Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLC) and others. A PCS consists of combinations of control components that act together to achieve water treatment and distribution objectives.

Risk: The calculated likelihood and impact of a threat exploiting a vulnerability.

Secure Token (ID Card, S-Key): A physical device used to gain access to an electronically restricted resource. The token is used in addition to or in place of a password. It acts like an electronic key to access a critical system network.

Security Patch: A piece of software designed and created to update a computer program or its supporting data, to fix or improve it. This includes fixing security vulnerabilities and other bugs, usually called bug fixes. Each patch is created to improve the usability and/or performance of the system or application.

Supervisory control and data acquisition (SCADA): A methodology involving equipment that both acquires data on an operation and provides limited to total control of the equipment in response to the data.

Threat: A possible danger that might exploit a vulnerability to breach security and therefore cause possible harm.

United States Computer Emergency Readiness Team (US-CERT): An organization within the Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD). Specifically, US-CERT is a branch of the Office of Cybersecurity and Communications (CS&C) National Cybersecurity and Communications Integration Center (NCCIC). US-CERT is responsible for analyzing and reducing cyber threats, vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

Virtual Private Network (VPN): A virtual private network (VPN) extends a private network across a public network, such as the internet. A VPN enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Virus: A hidden, self-replicating section of a computer software or program, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of another program. A virus cannot run by itself and requires that its host program be run to make the virus active.

Vulnerability: A weakness which can be exploited by an attacker, to perform unauthorized actions within a computer system.

Vulnerability assessment: The process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.

Vulnerability Management: The practice of identifying, classifying, prioritizing, remediating, and mitigating vulnerabilities.

Vulnerability scanning: An inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. A scan may be performed by an organization's IT department or a security service provider.

Water Information Sharing and Analysis Center (WaterISAC): An information sharing organization for the U.S. water and wastewater sector. WaterISAC helps its members strengthen their physical security and cybersecurity, recover from natural and man-made disasters and improve overall preparedness and resilience.

Whitelisting: A list of entities that are considered trustworthy and are granted access or privileges.

Appendix B – References and Resources

The following references and documents were utilized to develop the cybersecurity tools in this document:

- EPA Cyber Security 101 for Water Utilities, July 2012
- EPA Incident Action Checklist – Cybersecurity, October 2017
- EPA Water Sector Cybersecurity Brief for States
- New York State Department of Health Water Supply Vulnerability Assessment - Cybersecurity
- National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity", April 16, 2018
- WaterISAC 10 Basic Cybersecurity Measures - Best Practices to Reduce Exploitable Weaknesses and Attacks, October 2016
- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities – Best Practices to Reduce Exploitable Weaknesses and Attacks, 2019

Cyber Security Evaluation Tool (CSET®): Below is a link to a useful desktop software tool, that guides users through a step-by-step process to assess their control systems and information technology network security practices against recognized industry standards.

Department of Homeland Security, National Cybersecurity and Communications Integration Center's CSET®:

- CSET® Fact Sheet
- CSET® Software Download

The following references were utilized to assemble the Glossary of Terms:

- American Water Works Association, 2016, Water Distribution, Grade 3 & 4
- Cyber Glossary (Cyberpolicy.com)
- Cyber Security Glossary (Cybrary.it)
- Encyclopedia (PCMAG.com)
- Explore Terms: A Glossary of Common Cybersecurity Terminology (NICCS.us-cert.gov)
- Glossary of Identity and Cybersecurity Terms (The University of Texas at Austin, identity.utexas.edu)
- Malware: Viruses, Spyware, Adware & Other Malicious Software (UMass Amherst, www.umass.edu)
- What are malware, viruses, Spyware, and cookies, and what differentiates them? (Symantec.com)
- Wikipedia (Wikipedia.com)

Appendix C – Acknowledgements

"Cybersecurity Tools to Understand, Evaluate, and Mitigate Risks" was made possible by the generous support and funding provided by the Maine Drinking Water Program. In addition, the final version of this document was made possible after an in-depth review and pilot testing by several of Maine's PWS and IT/Cybersecurity professionals. We would like to acknowledge and recognize the following individuals for dedicating their valuable time, expertise and recommendations:

- Timothy Berger, Strategic Account Manager, Red Lion Controls, Inc.
- Robert Burke, Director of Water Treatment, Bangor Water District
- Eric Gagnon, Assistant Superintendent, Yarmouth Water District
- Devin Grady, Network Systems Administrator, Town of Gorham
- Kenneth Knight, Business Account Sales Executive, U.S. Cellular
- Robert MacKinnon, Superintendent, Yarmouth Water District
- Jason McLean, Information Security Analyst, Unlimited Technology
- Craig Starr, Information Technology Manager, City of Lewiston
- Amy Williams, Vice President of Cyber Services, PhD, CISSP