COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **LOW**

2.I: Does the WWS provide/conduct annual cybersecurity awareness training for all WWS personnel that covers basic cybersecurity concepts?

Recommendation: Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

Why is this control important?

To help create and maintain a culture of cybersecurity, your WWS should provide regular, basic cybersecurity training to all personnel. While cybersecurity covers many areas, there are certain basic security concepts that should be frequently emphasized to promote better cyber practices. Regularly trained personnel are more likely to identify and respond quickly to a potential cyber incident or prevent one from occurring altogether. Regular training is also critical as cybersecurity threats constantly evolve.

Implementation Tips

Establish a schedule to conduct regular training for all WWS personnel that covers basic cybersecurity concepts. The training should occur once per year, at a minimum.

Establish a policy that requires new employees to receive initial cybersecurity training within 10 days of onboarding. The training should consider the role of the new employee and cover basic security topics.

Additional Guidance

- ✓ Develop an agenda for the training to cover basic cybersecurity concepts, such as phishing, business email compromise, password security, latest trends and threats in social engineering, and best cyber hygiene practices. Social engineering is a common way to exploit people via social media (e.g., Facebook) and human interaction (e.g., email) to gain sensitive information and access. Use training concepts that are familiar to WWS staff, including real examples based on the equipment and systems used by the WWS. For example, if the WWS issues a smart phone to the employee, include specific training related to smart phone security. Since all staff probably receive email, the training should always include cybersecurity best practices for reviewing and opening email.

Additional Guidance (cont.)

- ✓ Develop the training materials so they are easy to follow and for personnel to reference later. Update PowerPoint presentations, online learning modules, and handouts for each training. Provide links to additional resources where WWS personnel can learn more about the cybersecurity topics. To keep cybersecurity relevant and fresh, consider adding a short cybersecurity segment to WWS staff meetings and briefings to share a quick tip or information related to cybersecurity.
- ✓ Staff that attackers commonly target, such as executives, executive assistants, engineers, SCADA staff, IT staff, operators, human resources, and finance personnel should receive more specialized training. Many free training opportunities are available online and in person, including from CISA and NICCS (see resources below).

Resources

EPA Cybersecurity Training for Water Systems
https://www.epa.gov/waterresilience/cybersecurity-training

WaterISAC's 15 Cybersecurity Fundamentals: Page 25 provides information for creating a cybersecurity culture at a WWS, including providing cybersecurity awareness training to all WWS staff.
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf

NIST Standard 800-16 and 800-50 Building an Information Technology Security Awareness and Training Program: Provides guidance for building an IT security awareness and training program. *https://csrc.nist.gov/publications/detail/sp/800-50/final*; *https://csrc.nist.gov/publications/detail/sp/800-16/final*

NIST Standard 800-82 Rev. 3 Guide to Operational Technology (OT) Security: Section 6.2.2 on page 108 provides OT training guidance. *https://csrc.nist.gov/pubs/sp/800/82/r3/final*

NIST Policy Template Guide: See Security Awareness and Training Policy. Contains Training schedules, records, slide decks, etc. demonstrating this training is conducted at least annually. *https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Awareness-and-Training-Policy.docx*

DHS CISA Training: Provides no cost online training on a variety of cybersecurity topics. *https://www.cisa.gov/cybersecurity-training-exercises*

DHS CISA Virtual Learning Portal: Provides no cost online training on a variety of cybersecurity topics. *https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA#need*

NICCS Federal Virtual Training Environment (FedVTE) Cybersecurity Training: Provides no cost online cybersecurity training for state, local, tribal, and territorial government employees. *https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte*

Stop Ransomware.gov: This is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively. *https://www.cisa.gov/stopransomware*

CISA's Top Cyber Actions for Securing Water Systems: See item 8 on page 3 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*