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

2.J: Does the WWS offer OT-specific cybersecurity training on at least an annual basis to personnel who use OT as part of their regular duties?

Recommendation: Provide specialized OT-focused cybersecurity training to all personnel who use OT assets.

Why is this control important?

The importance of regular basic cybersecurity training for all personnel is addressed in Factsheet 2.I. In addition, personnel who maintain or secure OT as part of their regular duties should receive OT specific cybersecurity training on at least an annual basis.

Implementation Tips

Identify the WWS personnel who should receive more specialized OT-focused cybersecurity training. At a minimum, WWSs should provide this specialized training to personnel who use OT assets as part of their regular duties.

Resources

CISA ICS Training: Provides no cost online training on a variety of OT security topics.
https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA

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

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

Additional Guidance

- ✓ The WWS's designated OT vendor may be capable of conducting OT-focused cybersecurity training for the WWS.
- ✓ Instead of one large training that covers many topics, a WWS should conduct multiple trainings scheduled periodically throughout the year to help break topics into short, digestible sessions.
- ✓ Develop the training agenda and materials so they are easy to follow and reference later. The training should cover OT asset security, configurations, safety functions, incident response actions, and general operations. If the WWS can operate manually without the use of OT, consider adding training for manual operations. Manual operations may be an essential line of defense in keeping the WWS operational in the event of a cyberattack. There are many online training opportunities available for WWS personnel, including those from CISA and NICCS (see resources).

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*

SANS Institute - Premier Hands-on ICS Training: This fee-based training offers several courses designed to increase the cybersecurity skills of those who use OT/ICS at their WWS. *https://www.sans.org/cyber-security-courses/?focus-area=industrial-control-systems-security&msc=main-nav*