`

COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

1.D: Does the WWS provide regular opportunities to strengthen communication and coordination between OT and IT personnel, including vendors?

Recommendation: Facilitate meetings between OT and IT personnel to provide opportunities for all parties to better understand organizational security needs and to strengthen working relationships.

Why is this control important?

It is critical that both OT and IT personnel, including vendors, understand each other's cybersecurity drivers, challenges, needs, and goals. Since separate departments often use OT and IT systems and separate staff or vendors maintain them, WWSs frequently manage the security of these systems separately. This separation can lead to gaps in security, especially with interconnected OT and IT systems. Regular coordination and communication between OT and IT cybersecurity personnel can help develop a more comprehensive approach to WWS cybersecurity.

Implementation Tips

Sponsor at least one collaborative meeting per year for OT and IT personnel. Finding a date and time that works for all parties can be difficult, so schedule the meeting well in advance. In-person meetings provide more relationship building opportunities.

A cybersecurity drill, or tabletop exercise, is an impactful way to bring together both OT and IT personnel, practice existing plans, policies, and procedures, and address security gaps based on exercise lessons learned. Including a few social breaks in the exercise can allow for relationship building.

Additional Guidance

- ✓ Vendor(s)/contractor(s) may require payment for their attendance at the meeting. Plan for this cost in the annual budget. You could schedule the meeting for the same day the vendor(s) is(are) planning to be at the WWS to conduct regular system maintenance.
- ✓ Develop and share an agenda in advance of the meeting to allow time for OT and IT personnel to prepare discussion points. Topics can include new WWS OT/IT hardware, firmware, and software updates; changes in network architecture; reports on updated plans, policies, or procedures; changes in personnel; roles and responsibilities; planned future cybersecurity activities; and emerging cybersecurity threats.
- ✓ Record action items from the meeting, including personnel responsible, so that you can check item status at regular intervals.

Resources

EPA Tabletop Exercise Tool: This tool helps WWSs to design their own exercises; a cybersecurity scenario is provided. *https://ttx.epa.gov/index.html*

CISA Tabletop Exercise Packages: These resources are designed to assist WWSs and others in conducting their own exercises. Note that under “Cybersecurity Scenarios” there is one for water systems. *https://www.cisa.gov/cisa-tabletop-exercise-packages*