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

**1.C:** Does the WWS have a named role/position/title that is responsible for planning, resourcing, and executing OT-specific cybersecurity activities?

**Recommendation:** Identify one WWS role/position/title responsible for ensuring planning, resourcing, and execution of OT-specific cybersecurity activities.

## Why is this control important?

WWSs should assign a named role/position/title the responsibility as lead for OT-specific cybersecurity activities. The person who fills this "OT cybersecurity lead" role/position/title should have oversight and authority for all OT-specific cybersecurity and be responsible for planning, resourcing, and execution of all OT-specific cybersecurity activities.

## Implementation Tips

Select a position within your WWS for the named role/position/title responsible for OT cybersecurity. This OT cybersecurity lead could be the same role/position/title named in 4.1, a different role/position/title at the WWS, a municipal or county level role/position/title, or the role/position/title overseeing a designated OT vendor who provides cybersecurity services. The OT cybersecurity lead may be different than the System Administrator. The OT cybersecurity lead could be the same role/position/title responsible for overall OT operations.

### Additional Guidance

- ✓ The OT cybersecurity lead should have a good working knowledge of how your WWS configures, uses, and maintains its OT systems. For example, you could name an employee who uses OT as part of their regular duties in the role/position/title.
- ✓ Establish and document clear tasks for the OT cybersecurity lead, such as adding these tasks to an existing position description. Include diagrams and photos where necessary.
- ✓ Identify any critical staff that should assist the OT cybersecurity lead.

If the OT cybersecurity lead will fully discharge their duties with no outside help, ensure that the employee in this role has sufficient training opportunities to effectively carry out their responsibilities. Include in performance reviews the execution of the responsibilities of OT cybersecurity lead. If a vendor will serve as the OT cybersecurity lead, the WWS should include language in the service level agreement/contract.

## Resources

**NCCIC's ICS Cybersecurity for the C-Level:** Provides examples of six cybersecurity risk oversight questions an OT cybersecurity lead should be asking about their organization's environment and includes services and practical action steps specific to critical infrastructure.
*https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_ICS_Cybersecurity_C-Level_S508C.pdf*

**NICCS's Workforce Framework for Cybersecurity (NICE Framework):** This resource helps employers develop their cybersecurity workforce. Review the "Cybersecurity Management" module. *https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cybersecurity-management*

**NIST Policy Template Guide:** See Account Management/Access Control Standard. A guide that utilities can use to assist them with account management and access controls.
*https://www.cisecurity.org/wp-content/uploads/2020/06/Account-Management-Access-Control-Standard.docx*