Identify: Asset Inventory

`

COST: **$$**$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

1.A: Does the WWS maintain an updated inventory of all OT and IT network assets?

Recommendation: Regularly review (no less than quarterly) and maintain a list of all OT and IT assets with an IP address. This includes third-party and legacy (i.e., older) equipment.

Why is this control important?

Your WWS cannot protect or secure what you do not know. An accurate inventory of both OT (e.g., SCADA, PLCs, HMIs) and IT (e.g., office computers, network switches, servers) technology assets is a critical part of WWS cybersecurity. Once your WWS knows what assets you have, you can make necessary cybersecurity improvements on the OT and IT networks.

Implementation Tips

There are several methods for inventorying assets, and the best approach is a combination of physical inspection, passive scanning, active scanning, and configuration (set up) analysis.

WWS should know what assets they have, how those assets are configured (see Factsheet 2.O), and how those assets are connected (see Factsheet 2.P).

Additional Guidance

- ✓ Based on the review, update out-of-date records for known assets, add previously unknown assets to the inventory, and delete any assets from the list that the WWS no longer uses.
- ✓ Ensure the list identifies physical assets and includes details for the assets, including how they are connected, what data they share, and who at the WWS (or what vendor) works with the asset.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control CM-8 (page 107) for more information on “System Component Inventory”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Information Security Policy (4.6) IT Asset Management. *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

SANS Institute Industrial Control System (ICS) Security Blog post “Know Thyself Better than the Adversary – ICS Asset Identification and Tracking”: Provides information on asset identification and tracking. *https://www.sans.org/blog/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking/*

`

WaterISAC's 15 Cybersecurity Fundamentals: See the section on page 7, "Perform Asset Inventories" for additional information. *https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf*

CISA's Top Cyber Actions for Securing Water Systems: See item 4 on page 2 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*