`

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

2.O: Does the WWS maintain current documentation detailing the set-up and settings (i.e., configuration) of critical OT and IT assets?

Recommendation: Maintain accurate documentation of the original and current configuration of OT and IT assets, including software and firmware version.

Why is this control important?

While your WWS may know the physical assets that exist on its computer networks from performing an asset inventory (see Factsheet 1.A), understanding the configuration (i.e., settings) of its assets is important as well. Attackers often exploit vulnerabilities (i.e., weaknesses) that only exist in certain versions or settings of the software and firmware used to control assets. Therefore, you should be aware of asset configurations to know whether a newly found vulnerability could be used in an attack on the network.

Additionally, if an attacker changes asset configurations, wipes settings, or disables assets, well-maintained configuration documentation will allow your utility to detect changes more easily, re-establish appropriate settings, and maintain or restore operations.

Implementation Tips

Review and update configuration documentation on a regularly scheduled basis.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control family CM-1 (page 96) and control CM-6 (page 103) for more information on “Configuration Management” and “Configuration Settings”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Information Security Policy (4.11b) System Security. A document that details asset configurations of OT and IT assets. *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

Additional Guidance

- ✓ To fully document asset configurations, include the following details, as applicable: owner (e.g., Engineering Department), physical and network location, vendor, asset type, model, asset name, firmware and/or software versions, patch levels, asset configurations, active services (i.e., automated processes), communication protocols, network addresses (e.g., IP and MAC), asset value, and criticality to WWS operations.
- ✓ To be efficient, a WWS can perform a review of its asset configuration at the same time as the asset inventory process detailed in Factsheet 1.A and the network survey detailed in Factsheet 2.P. Configuration information is important to preparing for or responding to a cyberattack; however, it would also be valuable to an attacker, so the WWS should protect it accordingly.