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

2.A: Does the WWS change default passwords?

Recommendation: When feasible, change all default manufacturer or vendor passwords before equipment or software is put into service.

Why is this control important?

Attackers can easily obtain default passwords from a product's user manual and use these credentials to gain access to systems either locally or across the Internet if the target system is connected. Off-the-shelf hardware and software are designed for easy installation and use. Factory default settings include simple, publicly documented passwords, such as "1111". Many times, these default passwords are identical (shared) among all systems from a vendor or within product lines.

Implementation Tips

Develop an enforced organization-wide policy and/or process that requires changing default vendor or manufacturer passwords for any hardware or software used at your WWS.

To enhance security and system integrity, WWSs may want to require that all vendors involved in the installation and configuration of hardware and software remove all default passwords and replace them with secure, unique credentials prior to system handover. This measure is essential to ensure that systems are protected against unauthorized access and to alleviate the need for staff to manage technical adjustments that require specialized knowledge.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: Provides a proactive and systemic approach to develop and make

Additional Guidance

✓ WWSs should review their existing asset inventory and identify any assets that have default passwords. These assets may include network hardware (e.g., network switches, wireless access points, network routers); communications assets (e.g., radios); OT assets (e.g., PLCs and HMIs); and software applications where the manufacturer or vendor installing the application at the WWS sets default passwords. Review the documentation for these assets, including instruction manuals and configuration guides (commonly available on the vendor's website), to identify any default usernames or passwords. The System Administrator should attempt to login using the default credentials and if successful, determine if the Administrator can change them without impacting system operations. In instances where changing default passwords is not feasible, implement and document appropriate compensating security controls and monitor logs for network traffic and login attempts on those assets. While changing default passwords on a WWS's existing OT may require support from a qualified vendor or integrator and may not always be feasible, the WWS should change default credentials for all newly deployed hardware or software.

`

available a comprehensive set of safeguarding measures for all types of computing platforms. See control IA-5 (page 138) for more information on "Authenticator Management". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Identification and Authentication Policy (1.b-1.d, 1.f). This policy details how many unsuccessful login attempts it takes to lock an account. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

DHS CISA Alert (TA13-175A): Issued in 2016, this alert describes why it is important to change the default password and provides mitigating actions. *https://www.cisa.gov/uscert/ncas/alerts/TA13-175A#:~:text=Attackers%20can%20easily%20identify%20and,to%20critical%20and%20important%20systems*.

CISA's Top Cyber Actions for Securing Water Systems: See item 3 on page 2 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*