Protect: Phishing-Resistant Multi-Factor Authentication (MFA)

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

2.H: Does the WWS require MFA wherever possible, but at a minimum to remotely access WWS Operational Technology (OT) / Information Technology (IT) networks?

Recommendation: Deploy MFA as widely as possible for both OT and IT networks. At a minimum, MFA should be used for remote access to the OT network.

Why is this control important?

MFA can prevent an attacker who acquires a user password from accessing critical WWS networks. MFA, also called two-factor authentication, requires WWS staff and other users to present at least two separate types of credentials when logging in to a WWS system. Credentials can be knowledge-based (like a password or PIN), asset-based (like a smart card or mobile phone), or biometric (like fingerprints). Credentials must come from two different categories – so entering two different passwords would not be considered MFA.

All remote users or vendors should require MFA to reduce risk. Many remote access applications and virtual private network (VPN) systems offer this capability or can be set up to offer this capability by using a third-party tool.

Implementation Tips

Within OT networks, enable MFA on all accounts and systems that the WWS can access remotely, including vendor/maintenance accounts, user and engineering workstations, and HMI applications.

Use MFA to verify the identity of a user where possible. Common MFA methods include biometrics, smart cards, FIDO/CTAP (client to authenticator protocol) enabled hardware assets, or one-time passcodes sent to or generated by previously registered assets like a mobile phone.

Additional Guidance

- ✓ Review any use of remote access, particularly to OT systems, and identify if the WWS can enable MFA on the software used for this access. There are several applications that can assist with enabling multi-factor authentication at a WWS. Some of the most popular include TeamViewer and Microsoft 365 for Windows. The resources section below provides links for setup.
- ✓ If the WWS cannot use MFA (such as some System Administrator, root, or service accounts), those accounts should use passwords that are unique to that one system and should not be accessible remotely where possible.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See page 132 “Identification and Authentication” for more information on MFA. *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) Identification and Authentication. An organization-wide policy and/or procedure requiring the use of MFA at a utility for remotely accessing the OT network. *https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-and-Authentication-Policy.docx*

Microsoft 365 Multi-factor Authentication Reference: This page describes how to configure multi-factor authentication settings on Microsoft 365 accounts. *https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide*

TeamViewer Authentication Reference: This page describes how to configure multi-factor authentication settings on the TeamViewer platform. *https://community.teamviewer.com/English/kb/articles/109255-enable-two-factor-authentication-enforcement-on-company-members*