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

2.V: Does the WWS prohibit the connection of unauthorized hardware (e.g., USB drives, removable media, laptops brought in by others) to OT and IT assets?

Recommendation: When feasible, remove, disable, or otherwise secure physical ports (e.g., USB ports on a laptop) to prevent unauthorized assets from connecting.

Why is this control important?

Only allowing authorized assets to connect your WWS networks helps stop attackers from getting into or stealing data from those networks.

Connecting a malicious USB asset to the WWS network can lead to system breach, disruption, or damage. The most well-known example of an attacker using a USB to damage an industrial plant is Stuxnet, the first publicly known malware designed to target OT systems. Even if your WWS does not connect a network to the Internet (e.g., an "airgap"), it could still be vulnerable to attacks from direct connections.

Implementation Tips

Disable AutoRun features that grant automatic access to removable media (e.g., USB drives) when connected to a computer.

Allow access to physical connection ports on computers only through approved exceptions.

Additional Guidance

- ✓ WWSs can stop the use of unauthorized assets by using physical cages to cover computer ports, through administrative policies (less effective), or by disabling technical permissions through an organization-wide policy within Microsoft Windows. If a WWS allows users to connect external assets to their systems, the WWS should check the assets for malware prior to connecting them. WWSs can generally configure anti-virus software to automatically scan external drives such as USBs when a user inserts them.
- ✓ If necessary, establish an administrative process where a user can request an exception to using an external asset by justifying the operational need. The relevant OT/IT personnel or System Administrator will need to weigh the operational need against the potential security risk to the WWS's computer system(s).

Resources

MITRE ATT&CK - Stuxnet: See "Replication Through Removable Media" for more information on Stuxnet's spread. *https://attack.mitre.org/software/S0603/*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control MP-7 (page 176) and SC-41 (page 326) for more information on "Media Use" and "Port and I/O Device Access". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Information Security Policy (4.6b) IT Asset a written administrative policy banning the use of USB drives and other removable media when appropriate**.** *https://www.cisecurity.org/wp-content/uploads/2020/06/Information-Security-Policy.docx*

Microsoft Learn - Enabling and Disabling AutoRun: See the section on "Using the Registry to Disable AutoRun" for more information. *https://learn.microsoft.com/en-us/windows/win32/shell/autoplay-reg#using-the-registry-to-disable-autorun*