Protect: Limit OT Connections to Public Internet

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

2.X: Does the WWS eliminate connections between OT assets and the Internet?

Recommendation: Eliminate OT asset connections to the public Internet unless explicitly required for operations.

Why is this control important?

Developers did not design SCADA and OT systems with cybersecurity in mind, and most WWSs do not patch or update them regularly. Directly connecting OT to the Internet can present a major cybersecurity risk to WWS operations. Your utility should know which SCADA or OT assets the WWS has connected to the Internet and remove the Internet connection if possible.

If operational needs require an internet connection (e.g., remote site management), you can reduce the cyber risk introduced by these connections through compensating controls like MFA, firewalls, and centralized logging.

Implementation Tips

Identify and disconnect all OT assets from the Internet. Check for standard connectivity (e.g., the SCADA network connected to the IT network or Internet modem) and other methods (e.g., wireless or cellular) for connecting OT assets to the Internet.

Your WWS should formally justify Internet connections to any OT assets and include compensating controls.

Additional Guidance

- ✓ As mentioned in Factsheet 2.W, a WWS can search for Internet-exposed OT assets by using Shodan or DHS CISA's free vulnerability scanning services. An example of an easily overlooked connection between OT systems and the Internet is the use of cellular modems to connect remote assets (e.g., tanks, lift stations, wells) to the primary SCADA system. When used, cellular modems should be on the telecom provider's private networks whenever possible.
- ✓ The WWS should create a process for justifying and documenting the operational need for an OT connection to the Internet with the OT cybersecurity lead. When operational needs require an approved OT connection to the Internet, the WWS should use the compensating controls detailed in Factsheet 2.W to mitigate the cyber risk this connection creates.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control AC-17 (page 48) and SC-7 (page 297) for more information on "Remote Access" and "Boundary Protection". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

DHS CISA Cyber Hygiene Services: See this resource for more information on DHS' free vulnerability scanning service. *https://www.cisa.gov/cyber-hygiene-services*

Shodan: See this resource to search for Internet-connected assets on the WWS's network. *https://www.shodan.io/*

CISA's Top Cyber Actions for Securing Water Systems: *See item 1 on page 1 of this resource for additional information. https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*