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

2.K: Does the WWS use effective encryption to maintain the confidentiality of data in transit?

Recommendation: When sending information and data, use Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption standards.

Why is this control important?

Encryption is the process by which computers convert information (e.g., files, network traffic) from "plain text" that people can read into an unreadable coded message. This step is important, as attackers will often attempt to intercept messages to alter commands to OT and IT assets and steal passwords or other sensitive information.

When you use encryption when sending information, and attackers intercept a message, they will not be able to use the information as it will be unreadable. This step helps to maintain the confidentiality (i.e., secrecy) of sensitive information and the integrity (i.e., correctness) of OT and IT information.

Implementation Tips

For OT and IT computer systems use encryption for communications with remote or external assets.

Update any weak or outdated data encryption software.

Additional Guidance

- ✓ TLS and SSL are the most common encryption protocols that systems use for sending information and data, and WWSs can configure assets such as desktops and servers to send and receive encrypted messages using one of these protocols. TLS is a newer and more secure alternative to SSL and is generally the preferred encryption standard if feasible. A WWS should perform a review of the current encryption protocol that it uses, compare this protocol to current standards, and develop a plan for improvement if necessary and operationally feasible.
- ✓ Configuration settings for encryption may be available for a variety of communications including remote access software, web-based HMI software, wireless communications (e.g., Wi-Fi), and radio communications. A WWS should encrypt and password-protect Wireless communications and avoid "open" (i.e., password-less) Wi-Fi networks. Virtual Private Networks (VPNs) for remote access into WWS systems and Cloud services for remote storage and application hosting will likely offer this capability by default.
- ✓ Within Windows, the WWS can enable TLS via the Configuration Manager. If implementing TLS via Windows Configuration manager, make sure to start with clients/endpoints (desktops and laptops). If starting implementation at the server-level, it may cut off communication to client assets.

`

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-8 (page 304) for more information on "Transmission Confidentiality and Integrity." *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

NIST Policy Template Guide: See Encryption Standard (4.1) Data in Transit. Documented SOP for encryption that can be included in the utility's cybersecurity policy**.** *https://www.cisecurity.org/wp-content/uploads/2020/06/Encryption-Standard.docx*

Microsoft Core Infrastructure Guide: See the links below for instructions on how to enable TLS 1.2 on clients (e.g., desktops and laptops) and servers via Windows Configuration Manager.

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2-client

https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2