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

2.Q: Does the WWS require approval before new software is installed or deployed?

Recommendation: Only allow Administrators to install new software on a WWS-issued asset.

Why is this control important?

Permitting only approved software on your WWS assets, preferably installed by an Administrator, allows your utility to ensure that software is free of malicious code prior to installation. Users can utilize software to perform normal business activities or for malicious purposes intended to harm the computer system and/or business. An attacker may disguise malicious software as normal software to mislead a user into installing it, such as advertising legitimate features without disclosing malicious features or by mimicking the style and/or web address of a reputable vendor's download portal.

If a WWS employee intentionally or unintentionally installs malicious software, the WWS could be vulnerable to system breach, disruption, or damage.

Implementation Tips

Establish controls for WWS-issued computers and other assets to restrict the software that users can install.

- Examples include restricting administrative privileges (i.e., only certain designated individuals can install software on a WWS's computers, such as a System Administrator) or only allowing approved software downloads.

Additional Guidance

✓ A WWS can manage software made available to staff through a download portal on each asset (e.g., Windows Software Center) or more simply from a list of approved software. To install new software, a WWS employee should submit a request to the OT/IT personnel or the System Administrator justifying the operational need for the new software.

Implement a process that requires approval before users can install new software or software versions.

Maintain a risk-informed list of allowed WWS software, including specification of approved versions where technically feasible.

Resources

GAO-22-104746 - Federal Response to SolarWinds and Microsoft Exchange Incidents: See the "What GAO Found" section for more information on the 2020 SolarWinds Supply Chain Attack. *https://www.gao.gov/products/gao-22-104746*

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control CM-11 (page 112) for more information on "User-Installed Software". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn - Software Center User Guide: See this resource for more information on how to plan for and configure Microsoft Software Center. *https://learn.microsoft.com/en-us/mem/configmgr/apps/plan-design/plan-for-software-center?source=recommendations*