Identify: Vendor/Supplier Cybersecurity Requirements

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

1.I: Does the WWS include cybersecurity as an evaluation criterion for the procurement of OT and IT assets and services?

Recommendation: Include cybersecurity as an evaluation criterion when procuring assets and services. Where feasible, seek out systems that are secure by design and secure by default.

Why is this control important?

Implementing this control will help the WWS to buy more secure products and services, reducing cyber risk. Granting a vendor access to your network to perform a service (e.g., maintenance, configuration changes) or install new hardware or software can add a new way for attackers to breach the network. If a vendor remotely accesses your utility network without effectively securing its own computer systems, any malware or infections on the vendor's systems can migrate onto WWS systems.

Installed hardware or software may have unintentional weaknesses (i.e., vulnerabilities) that an attacker can use to enter a system. Further, an attacker (with or without the knowledge of the vendor) can intentionally insert vulnerabilities into hardware or software to introduce a weakness to the WWS network. The 2020 SolarWinds Attack is an example of such an attack that affected several Federal Government agencies.

Concerns that foreign governments could intentionally place weaknesses in hardware products exported from their country has led the Federal Communications Commission to ban certain vendors from U.S. Federal Government networks as well as from importation and sale in the U.S.

Implementation Tips

Insert cybersecurity requirements in the procurement process at the earliest stage so that vendors responding to the bid request will know to include these requirements up-front. Your WWS should require vendors to use secure techniques such as a Virtual Private Network (VPN) and MFA when accessing your network remotely. The Department of Energy resource below provides example procurement language for vendor cybersecurity requirements that WWSs can insert into vendor contracts.

Additional Guidance

- ✓ Given two offerings of roughly similar cost and function, the WWS should give preference to the more secure offering and/or supplier.
- ✓ The WWS can also implement firewalls to filter out unusual traffic as well as monitor and log network activity.

To evaluate hardware and software vendors and reduce the cyber risk they present to your assets, ask vendors about their cybersecurity practices and research them online to get a sense of their overall cyber safety. Use government advisories to research potential vendors and search vulnerability databases (i.e., the Known Exploited Vulnerabilities (KEV) and National Vulnerability Database (NVD)) (See Factsheet 1.E).

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SR-6 (page 369) and SR-5 (page 368) for more information on “Supplier Assessments and Reviews” and “Acquisition Strategies, Tools, and Methods”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

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*

DHS CISA Known-Exploited Vulnerabilities (KEV): See this resource for vulnerabilities that attackers have already used. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

NIST National Vulnerability Database (NVD): See this resource for a list of publicly known vulnerabilities. *https://nvd.nist.gov/vuln/search*

FCC – Enacted Vendor Hardware Bans: See these resources for details on current bans of vendor hardware.

https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats

https://www.fcc.gov/document/fcc-bans-authorizations-devices-pose-national-security-threat

Department of Energy (DOE) Cybersecurity Procurement Language: See this resource for example cybersecurity procurement language to include in vendor contracts. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA’s National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*