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

1.G/1.H: Does the WWS require that all OT and IT vendors and service providers notify the WWS of any security incidents or vulnerabilities in a risk-informed timeframe?

Recommendation: Require vendors and service providers to notify the WWS of potential security incidents and vulnerabilities within a stipulated timeframe described in procurement documents and contracts.

Why is this control important?

Receiving timely notification of vendor security incidents and vulnerabilities gives your WWS the opportunity to prevent or respond to potential attacks.

Implementation Tips

Your utility should include a contractual notification requirement in procurement documents for hardware and software products and Service-Level Agreements (SLAs) for services. You can choose a reasonable, risk-informed timeframe for the vendor to notify your WWS of newly discovered vulnerabilities in a vendor's offerings and cyberattacks on the vendor's computer systems. Include clauses requiring these notification timeframes in future procurement contracts and SLAs with vendors as well as the penalties if the vendor does not meet these requirements.

Additional Guidance

- ✓ When reviewing cybersecurity requirements within contracts, review both service provider contracts and hardware/software vendor agreements (e.g., OT integrator, IT vendor).

The Department of Energy resource below provides example procurement language for vendor cybersecurity requirements that WWSs can insert into vendor contracts.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SR-8 (page 371) for more information on "Notification Agreements". *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*

Department of Energy (DOE) Cybersecurity Procurement Language: See section 3.3 on "Problem Reporting" within this resource for example cybersecurity language to include in vendor contracts. *https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014*