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

4.A: Does the WWS have a written procedure for reporting cybersecurity incidents, including how (e.g., phone call, Internet submission) and to whom (e.g., FBI or other law enforcement, CISA, state regulators, WaterISAC, cyber insurance provider)?

Recommendation: Document the procedure for reporting cybersecurity incidents promptly to better aid law enforcement, receive assistance with response and recovery, and to promote water sector awareness of cybersecurity threats.

Why is this control important?

Reporting incidents to outside agencies can help WWSs better respond to and recover from a cybersecurity incident. Reported information may also help stop the cybercrime from occurring at other WWSs and organizations as well as provide trend information and awareness to the water sector.

Implementation Tips

Develop a procedure and report template for reporting cybersecurity incidents promptly.

Identify the WWS personnel responsible for reporting to external organizations.

Specify escalation procedures (e.g., who to notify) for reporting to the identified external organizations and the timeframes for reporting information. Flow diagrams or other visuals can help WWS personnel to understand in what order they should notify others and what information they should report.

Distribute the reporting procedure and template to WWS personnel. Include this information in other emergency response documents, like your emergency response plan or cybersecurity incident response plan.

Under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is required to issue regulations, through notice-and-comment rulemaking, requiring covered entities to report covered cyber incidents and ransom payments made as a result of a ransomware attack to CISA. CISA's Notice of Proposed Rulemaking proposes applying these requirements to at least some entities in the WWS. EPA will revise this guidance as necessary when CISA issues the CIRCIA Final Rule. If the WWS subscribes to cyber insurance or has a cyber incident response retainer, include these providers as contacts within the written procedure. There are often required reporting timeframes associated with making claims against cyber insurance or incident response retainers.

Additional Guidance

The written procedure should include contact information for reporting to the following:

- The WWS's local law enforcement agency.
- DHS CISA–organizations should submit an online CISA incident report, send an email to report@cisa.gov, or call 888-282-0870.
- The Federal Bureau of Investigation (FBI)–organizations should contact their nearest FBI field office or submit a report through the Bureau's Internet Crime Complaint Center (IC3).
- The WaterISAC and local/state fusion centers–to report to WaterISAC, the WWS can submit an online WaterISAC report, email analyst@waterisac.org, or call 866-426-4722.
- The WWS's cyber insurance provider or cyber incident response retainer holder (if applicable).

The report template should include the following:

- Date and time when the WWS detected the incident
- Date and time when the incident occurred
- Brief description of incident including identification of potential attack method
- List of impacted assets
- Identification of any personally identifiable information (PII) that the incident may have compromised
- Date, time, and description of response/corrective actions that the WWS completed
- WWS personnel/vendor(s) involved in incident detection and response

Information that the WWS shares with DHS or FBI, or any other federal government agency, may be eligible for protection under the protected critical infrastructure information (PCII) program. For more information on what may qualify for PCII protection and procedures to follow to seek PCII protection, see CISA's PCII Factsheet.

Resources

Report to DHS CISA: Provides information on how to report incidents and suspicious activity. *https://www.cisa.gov/report*

Report to the FBI: Provides information on how to report cybercrime reports. *https://www.fbi.gov/investigate/cyber*

Report to WaterISAC: Provides information on how to report incidents and suspicious activity. *https://www.waterisac.org/report-incident*

NIST Policy Management Template Guide: See SOP and report template for reporting cybersecurity incidents that is distributed to all utility personnel. *https://www.cisecurity.org/wp-content/uploads/2020/06/Computer-Security-Threat-Response-Policy.docx*

DHS CISA's PCII Factsheet: Explains the protections offered by the PCII program. *https://www.cisa.gov/publication/pcii-fact-sheet* and *https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program/submit-critical-infrastructure-information*

DHS CISA Cyber Incident Response Factsheet: This guide can be used to help augment incident response planning and collaborate with federal partners. *https://www.cisa.gov/sites/default/files/2024-01/WWS-Sector_Incident-Response-Guide.pdf*