COST: **$**$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

5.A: Is the WWS capable of safely and effectively recovering from a cybersecurity incident?

Recommendation: Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.

Why is this control important?

Contingency planning for WWS OT and IT systems is part of an overall program for achieving continuity of operations for utility mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when OT and IT systems are compromised or breached.

Implementation Tips

Coordinate and test contingency plan development with utility departments responsible for related plans (e.g., WWS ERP).

Ensure needed capacity for information processing, telecommunications, and operations support exists during OT and IT outages.

Plan to resume essential mission and business functions within a defined time from contingency plan activation and test this response time.

Plan to continue essential mission and business functions with minimal or no loss of operational continuity and sustain that continuity until all OT and IT systems are fully restored.

Coordinate and test your contingency plan with the contingency plans of external service providers (e.g., SCADA vendor) as applicable to ensure that contingency requirements can be satisfied.

Additional Guidance

- ✓ Develop a contingency plan that:
  - Identifies WWS essential mission and business functions and associated contingency requirements
  - Provides recovery objectives, restoration priorities, and metrics
  - Addresses contingency roles, responsibilities, assigned individuals with contact information
  - Addresses maintaining essential mission and business functions despite an OT or IT system disruption, compromise, or failure
  - Addresses eventual, full system restoration
  - Addresses the sharing of contingency information
  - Is reviewed and approved by the WWS Cybersecurity Lead
- ✓ Distribute copies of the contingency plan as needed.
- ✓ Coordinate contingency planning activities with incident handling activities.
- ✓ Review the WWS contingency plan at a set frequency.
- ✓ Incorporate lessons learned from contingency plan testing, training, or implementation into the plan.
- ✓ Protect the contingency plan from unauthorized disclosure and modification.

Identify critical WWS OT and IT assets supporting essential mission and business functions (see Factsheet 1.A).

Resources

EPA Cybersecurity Incident Action Checklist: This checklist outlines actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents. *https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf*

EPA Cyber Incident Response Template: This customizable template can be used as a starting point for building your utility's Cybersecurity Incident Response Plan designed to help your utility respond to a cyber incident.
https://www.epa.gov/waterresilience/cybersecurity-planning

NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations: This publication provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, and other organizations from a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks. See section 3.6 Contingency Planning and Table C-6 Contingency Planning Family.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Incident Response Training: CISA offers Incident Response (IR) training courses free to government employees and contractors across federal, state, local, tribal and territorial government, educational and critical infrastructure partners, and the general public.
https://www.cisa.gov/incident-response-training

DHS CISA Cyber Incident Response Guide: 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

WaterISAC's 15 Cybersecurity Fundamentals: See Fundamental 11 on page 35, "Plan for Incidents, Emergencies and Disasters" for additional information.
https://www.waterisac.org/system/files/articles/15%20Cybersecurity%20Fundamentals%20%28WaterISAC%29.pdf