Drinking Water and Wastewater Systems Cybersecurity Incident Response Plan Template Instructions

EPA Office of Water (4608T) EPA 810-F-25-017 April 2025

Introduction

This template, developed by the U.S. Environmental Protection Agency (EPA), assists drinking water and wastewater systems with developing a Cybersecurity Incident Response Plan (CIRP). To access the CIRP template, click on the Word document icon to the right.

A CIRP describes your utility's strategies, resources, plans, and procedures to prepare for and respond to a cybersecurity incident that threatens life, property, or the environment. A CIRP supplements your utility's Emergency Response Plan.

When a cybersecurity incident occurs that requires a response, you will need to activate the procedures and protocols described in your CIRP. This can include implementing personnel emergency roles and responsibilities, and notifying external contractors (e.g., Operational Technology (OT) and Information Technology (IT) vendors) and others such as your local law enforcement and state regulatory agencies.

As you respond to an incident, you should immediately begin documenting your decisions, actions, and expenditures. This step is important for justifying incident costs and potentially seeking reimbursement once the incident is resolved and a claim is filed with your cybersecurity insurance provider. Good incident documentation involves creating a paper trail for receipts, records, photographs, and personnel timesheets.

For more information and resources related to cybersecurity for utilities, please visit the EPA Cybersecurity for the Water Sector website.

How to use this Template

This customizable template is designed to help your system respond to a cybersecurity incident and can be used as a starting point for building your utility's CIRP. Since each utility's OT and IT systems are unique, feel free to delete template sections or include additional sections with information tailored to your system's specific needs.

Throughout the template, bracketed, italicized text is explanatory text only. Text both bracketed and highlighted in yellow is to be accepted/updated as you develop your CIRP. Before starting your CIRP, save the CIRP template to your computer, delete the first page, delete bracketed and italicized instructional text, update bracketed and highlighted yellow text, and follow the steps below to gather the key information you'll need to develop or update your CIRP:

1. **Conduct a Risk and Resilience Assessment (RRA) on your OT and IT systems:** The findings and countermeasures identified in your RRA should be incorporated into your CIRP[1]. If your utility would prefer to have assistance assessing its cybersecurity preparedness, consider participating in EPA's Water Sector Cybersecurity Evaluation Program. Under this program, EPA will conduct a free cybersecurity assessment using EPA's Cybersecurity Checklist for Drinking Water and Wastewater Systems to identify cybersecurity gaps and vulnerabilities. Utilities that participate in the program will receive

[1] American's Water Infrastructure Act (AWIA) Section 2013 amends Section 1433 of the Safe Drinking Water Act, requiring community water systems serving more than 3,300 people to develop or update risk and resilience assessments and emergency response plans.

an Assessment Report and Risk Mitigation Plan in a secure file that can be added to their RRA and used to help develop the CIRP.

2. **Identify state regulatory and other requirements:** Many states have privacy laws governing the protection of personally identifiable information (PII). These requirements, as well as others relevant to preparing for, responding to, and recovering from a cybersecurity incident, should be incorporated into the CIRP.
3. **Identify and integrate existing plans and documents:** Your CIRP should align with other plans, policies, and procedures at your utility as much as possible. These may include an Emergency Response Plan (ERP), communication plans, emergency operations plans, inventory lists, network diagrams, and configuration settings.
4. **Coordinate with external contractors:** External contractors, such as vendors, third-party suppliers, and integrators, should be included in developing the CIRP, as they will be key response partners.
5. **Planning for cybersecurity incident response:** Planning for a cyber incident involves a structured approach to mitigate risks, respond effectively, and recover from incidents. As you develop your CIRP, you may find you need to document processes, gather information from contractors, and implement mitigation measures. More information about how to prepare your cybersecurity response program is provided in Appendix I.

See Appendix II for common terms and acronyms used in these instructions and the CIRP template. Appendix III outlines potential roles and responsibilities that can be implemented in the CIRP. Appendix IV provides information about cybersecurity incident types that should be reviewed as you develop your CIRP. Appendix V provides additional resources and references that you can use while developing your CIRP.

Once the CIRP is developed, it should be stored securely as it may contain sensitive information. Print and provide physical copies of the CIRP to all personnel involved in the incident response and recovery process, including any OT and/or IT Contractors. Consider storing one copy on-site and one copy off-site in case you are unable to access your facilities during an incident. You may also want to store an electronic copy on a shared drive or other digital platform (protected by a firewall) that is easily accessible.

Your CIRP should be viewed as a living and evolving document with established maintenance guidelines for routine and non-routine updates. These guidelines outline the circumstances under which updates will occur and specify the personnel or departments responsible for the updates.

Lastly, once your CIRP is complete, consider training your personnel and response partners on its contents and their individual roles and responsibilities. A multi-year training and exercise plan can help you schedule periodic trainings for both experienced and new personnel to help ensure that your CIRP procedures will be effectively implemented during an actual response. Tabletop exercises are also an effective means to practice and test your response procedures. Access EPA's Tabletop Exercise Tool to learn more. The EPA also offers free cybersecurity tabletop exercises for water and wastewater utilities to test incident response procedures and provide resources for developing and improving incident response plans. EPA partners with primacy

agencies, state agencies, water sector associations, Water and Wastewater Agency Response Networks (WARNs), CISA, and FBI to offer these tabletop exercises. Email watercyberta@epa.gov to request a tabletop exercise.

Table of Contents

PLAN INFORMATION

This section in the CIRP is to ensure that your utility's CIRP is reviewed and acknowledged accordingly, and all modifications are documented. Assign an Incident Response Lead and Incident Response Team. If your utility cannot staff an Incident Response Team, designate one individual as the Incident Response Lead who can also perform the functions of the Incident Response Team. Refer to Appendix III for a recommended list of responsibilities for the Incident Response Lead and other response roles.

i. Plan Approval

The CIRP should be reviewed and approved by the Incident Response Lead. By approving the document, the Incident Response Lead is acknowledging their responsibility for managing any cybersecurity incident. Anytime the CIRP is updated, the Incident Response Lead should review and acknowledge the latest version.

ii. Revision History

Document the plan's revision history so that all CIRP users can ensure they have the most up to date, approved version of the CIRP.

iii. Plan Distribution

The CIRP is distributed to all users of the plan, including members of the Incident Response Team, and other internal and external personnel. When changes to the CIRP are made and approved by the Incident Response Lead, document the distribution of the revised plan.

1.0 PURPOSE

This section provides information about the purpose of the CIRP. Your utility will reference other existing plans, policies, procedures, and documents that will help you respond to and recover from a cybersecurity incident. Examples of existing documents that may be useful to reference include the utility's ERP, external communications plan, network topology diagram, cybersecurity insurance policy, and contractor/vendor contract documents.

2.0 INCIDENT HANDLING PROCESS

This section should contain the actions your utility will take both during and after a cyber incident. Recommended actions are already provided in the tables that correspond to the incident management steps: identification, containment, eradication, recovery, and lessons learned. However, these listed actions may not all apply to your utility or there may be other actions that would apply specifically to your utility. Update the actions in the provided tables accordingly.

Another resource that can help you develop your CIRP is EPA's Cybersecurity Incident Action Checklist, a rip-and-run style checklist with actions for utilities to take to prepare, respond to , and recover from a cybersecurity incident.

2.1. Identification

When an abnormality or deviation from normal OT or IT operations is detected, a cybersecurity incident is likely occurring. The actions included in this table should be taken to better identify the type of incident, its potential origin, and the affected utility system(s).

2.2. Containment

Once an incident is identified, it must be contained before it spreads further across utility networks and causes more damage. The actions included in this table should be taken to contain the incident.

2.3. Eradication

Once an incident is contained, any resulting effects (e.g., breached user accounts) must be eradicated from infected utility systems. The actions listed in this table should be taken to remove any malware, corrupted files, and other changes resulting from the incident.

2.4. Recovery

Once eradication is complete, the actions in this table should be taken to restore utility systems and operations back to normal.

2.5. Lessons Learned

Documenting lessons learned from each cyber incident and performing follow-up corrective actions will enhance resilience and response efforts. Once an incident is closed, the actions included in this table should be taken to debrief from the incident, review lessons learned, and update the CIRP and any other policies and procedures as needed.

3.0 CONTACT LIST

Communication during an incident is crucial for relaying information to personnel, contractors, response partners, the public, and others about potential risks to data, health, and the environment. This section provides the key points of contact for response and recovery, along with their contact information. Identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include these contacts and their contact information in this table. You should include in this list any internal staff and external response partners, including contractors/vendors, government agencies, law enforcement, and media partners.

4.0 INCIDENT DATA COLLECTION

It is critical to document incident data for reporting and sharing with external response partners. Documenting incident information is also required for most cybersecurity insurance policies. This section includes an example form for the utility to document key information about the incident. Update this form based on your utility's specific needs.

5.0 APPLICABLE REGULATIONS AND REQUIREMENTS

Your utility may be required to comply with privacy laws and other cybersecurity regulations. Most states have laws that specify how to protect and manage PII. These legal requirements should be documented for easy reference in the event of an incident. If your system has a cybersecurity insurance policy, you may also need to comply with specific incident-handling requirements as described by your insurance provider. Ensure that you document any legal or other requirements that impact the way you prepare for and manage a cybersecurity incident.

6.0 TESTING AND UPDATES

Reviewing and testing the CIRP and making any necessary updates as needed will keep the plan relevant and effective. Update this section with any specific plans to keep your CIRP updated.

APPENDIX I – PLANNING FOR CYBERSECURITY INCIDENT RESPONSE

To prepare your utility to respond to a cybersecurity incident, it is essential to implement the priority cybersecurity mitigation actions outlined in EPA's Emergency Response Plan template, as detailed in the Checklist of Priority Cybersecurity Practices (see Section 3.2 of EPA's ERP template).

In addition to implementing the priority cybersecurity mitigation actions, you may consider implementing the following actions to develop your cybersecurity incident response program further:

1. Identify and catalog all mission-critical OT and IT systems, considering business enterprise, process control, and communications. Document the key functions of the mission-critical systems and identify the personnel or entity responsible for operating and maintaining each system. Appendix A to the CIRP template provides an outline to document this information. If this information is maintained in other utility documents, reference those documents in the table in Section 1.0 of the plan.
2. Document and map network data flows and access points to and from critical systems. Include a reference to this document in the table in Section 1.0 of the plan.
3. Catalog all OT systems configured for remote access and document the staff members who have remote access privileges to these systems. Include a reference to this document in the table in Section 1.0 of the plan.
4. Conduct frequent cybersecurity assessments to identify and address existing gaps or vulnerabilities. Below are two free cybersecurity assessment programs:
    a. EPA – Water Sector Cybersecurity Evaluation Program
    b. CISA - CISA's Free Cyber Vulnerability Scanning for Water Utilities
5. Conduct annual training with staff to ensure that mission critical functions can be performed. For example, train on manual operation of water collection, storage, treatment, and conveyance systems without OT.
6. Conduct drills and exercises for responding to a cyber incident. Below are three free cyber incident response training exercise resources:
    a. EPA's Tabletop Exercise Tool for Drinking Water and Wastewater Utilities helps utilities self-evaluate and strengthen their incident response capabilities. The tool includes a cybersecurity module and allows users to customize exercise details and generate a presentation to guide conducting their own tabletop exercise. It supports planning, facilitates discussion, and helps identify gaps in preparedness.
    b. EPA also conducts free cybersecurity tabletop exercises for water and wastewater utilities to test incident response procedures and to provide resources to develop and improve incident response plans. EPA partners with primacy agencies, state agencies, water sector associations, Water and

Wastewater Agency Response Networks (WARNs), CISA, and FBI to offer these tabletop exercises. Email watercyberta@epa.gov to request a tabletop exercise.

c. CISA's Tabletop Exercise Packages include cybersecurity-based threat vector topics including ransomware, insider threats, phishing, and Industrial Control System compromise, featuring a Water and Wastewater Systems Situation Manual.

7. Register for cybersecurity alerts and advisories. Below are a few sources of cybersecurity alerts:
    a. EPA – Water Sector Alerts
    b. CISA - Cybersecurity Alerts & Advisories
    c. CISA - Known Exploited Vulnerabilities Catalog
    d. MS-ISAC – Cybersecurity Threat Advisories
    e. WaterISAC – All-threats security information source for utilities
8. Set up an automatic backup for critical systems and ensure the process produces a readable, uncorrupted restore file on a routine basis.
9. Ensure logging is enabled on critical systems.
10. Meet your CISA state and regional team and your local law enforcement agency.
11. Create and implement comprehensive cybersecurity policies that address measures such as:
    a. Acceptable use of utility resources
    b. Data security and privacy
    c. Password management and security
    d. Third-party contractor/vendor security requirements
12. Define security standards and guidelines for all systems, applications and networks within the utility. Implement security controls to meet these standards, such as firewalls, antivirus software, and intrusion detection systems.
13. Establish clear reporting procedures for utility personnel to report suspected cybersecurity incidents to the Incident Response Lead.
14. Establish clear reporting procedures to external entities to report suspected cybersecurity incidents.
15. Disconnect all OT and IT system components to the Internet unless absolutely necessary. For OT systems that cannot be disconnected due to operational requirements, develop contingency measures such as alternate operational modes (e.g., manual operations) or fail-safe configurations.

APPENDIX II – ACRONYM LIST

Term	Definition
AAR	After Action Report
CIRP	Cybersecurity Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
HVAC	Heating, Ventilation, and Air Conditioning
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NGAV	Next-Generation Antivirus
OT	Operational Technology
PII	Personally Identifiable Information
SAFE	Security Assessment at First Entry
SOC	Security Operations Center
WARN	Water/Wastewater Agency Response Network
WaterISAC	Water Information Sharing and Analysis Center

APPENDIX III – POTENTIAL ROLES AND RESPONSIBILITIES

The Incident Response Lead is responsible for:

- Making sure that the Cybersecurity Incident Response Plan is current, reviewed and tested at least once each year.
- Maintaining access to an electronic and physical copy of the Cybersecurity Incident Response Plan.
- Making sure that staff with Cybersecurity Incident Response Plan responsibilities are aware of their role and responsibilities and are properly trained accordingly at least once each year.
- Leading the investigation of a suspected breach or reported cybersecurity incident and initiating the Cybersecurity Incident Response Plan when needed.
- Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as required.
- Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any cybersecurity incident investigation. This includes authorizing access to/removal of evidence from site.
- Developing organizational policies and procedures related to incident response.
- Identifying operational impacts to the organization in the event of an incident.
- Acting as an expert resource on cybersecurity threats and vulnerabilities.
- Understanding or delegating safeguards for OT systems.
- File a claim with the cybersecurity insurance provider, as applicable.

Incident Response Team members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual cybersecurity incident.
- Advising the Incident Response Lead of an incident when they receive a cybersecurity incident report from staff.
- Acting as the point of contact for all internally reported incidents or suspected incidents.
- Investigating and documenting each reported cyber incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering forensic information to support analysis and any legal actions.
- Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken during the response.
- Assisting law enforcement during the investigation process. This includes any forensic investigations and prosecutions.
- Initiating follow-up actions to reduce the likelihood of recurrence.
- Leading cyber exercises for the utility based on the determined frequency.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future.

OT/IT Operations and Support Staff are responsible for:

- Privilege management, enterprise password protection, and role-based access control.
- Discovering, auditing, and reporting on all privileged account usage.
- Conducting random checks to audit privileged accounts, validating whether they are required, and re-authenticating those that are.
- Monitoring privileged account uses and proactively checking for indicators of compromise, such as excessive logins or other unusual behavior.
- Informing the Incident Response Team of potential attacks that compromise privileged accounts, validating and reporting on the extent of attacks.
- Taking action to prevent the spread of a breach by updating privileges.
- Managing access to systems and applications for internal staff and partners.
- Centrally managing patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.
- Providing security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.
- Providing security bulletins and technical guidance to external users in case of a breach.

Technical Partners (e.g., contractors) are responsible for:

- Security controls to limit the progression of a cyberattack across third-party systems and organizations.
- Coordinating with the Incident Response Team to manage risks.
- Assisting with cyber incident prevention and recovery.

State and Local Government Regulatory Agencies are responsible for:

- Receiving necessary information about a cyber incident according to timeline and format mandated by state and local regulatory requirements.

Federal Threat Response (i.e., FBI) is responsible for:

- Conducting appropriate law enforcement and national security investigative activity at the affected water and/or wastewater system's site.
- Collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.

Federal Asset Response (i.e., DHS CISA) is responsible for:

- Furnishing technical assistance to affected water and wastewater entities to protect their assets, mitigate vulnerabilities, and reduce the impacts of cyber incidents.
- Identifying other water and wastewater utilities that may be at risk and assessing their risk to the same or similar vulnerabilities.

- Evaluating potential risks to the water sector or region, including potential cascading effects, and developing courses of action to mitigate these risks, facilitating information sharing and operational coordination with threat response.
- Guiding how best to utilize federal resources and capabilities in a timely, effective manner to speed recovery.

The Sector Risk Management Agency (i.e., EPA) is responsible for:

- Ensuring the utility receives the necessary support at the federal level to recover from the incident.
- Coordinating with the FBI, DHS CISA, state and local government, and the utility to capture and document detailed information about the incident and to confirm that the appropriate federal agencies are involved in the incident response process.
- Collaborates directly with the utility or indirectly through the state and local government, FBI, and DHS CISA to determine if there was an impact on water/wastewater production/treatment.
- Providing technical assistance and tools to assist the utility in preparing for a cyber incident.

Utility Legal Counsel (if available) are responsible for:

- Confirming requirements for informing employees, customers, and the public about cyber breaches.
- Checking in with local law enforcement.

Utility Audit & Compliance (if available) are responsible for:

- Communicating with regulatory bodies, following mandated reporting requirements.

Utility Human Resources (if available) are responsible for:

- Coordinating internal employee communications regarding breaches of personally identifiable information (PII) and responding to questions from employees.

Utility Marketing and Public Relations (if available) are responsible for:

- Communicating externally with customers, partners, and the media.
- Coordinating all communications and requests for interviews with internal subject matter experts and Incident Response Team.
- Maintaining draft crisis communications plans and statements that can be customized and distributed quickly in case of a breach.

Utility Web and Social Media Lead (if available) is responsible for:

- Posting information on the utility website, email, and social media channels regarding the cyberattack, including utility response and recommendations for customers.
- Monitoring across social media channels to ensure utility receives feedback or questions sent by customers through social media.

APPENDIX IV – COMMON INCIDENT TYPES

Type	Description
Unauthorized Access or Usage	An attacker gains physical or logical access to network, system, or data without permission.
Service Interruption or Denial of Service	An attack that prevents service access or otherwise impairs normal operation.
Ransomware Attack	An ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Attackers then demand ransom in exchange for decryption.
Malicious Code	Installation of malicious software (e.g., virus, worm, Trojan, or other code).
Network System Failures (widespread)	An incident affecting the confidentiality, integrity, or availability of networks.
Application System Failures	An incident affecting the confidentiality, integrity, or availability of applications or systems.
Unauthorized Disclosure or Loss of Information	An incident affecting the confidentiality, integrity, or availability of data.
Privacy Breach	Incident that involves real or suspected loss of personal information (e.g., staff social security numbers).
Information Security/Data Breach	Incident that involves real or suspected loss of sensitive information.

APPENDIX V – RESOURCES AND REFERENCES

Environmental Protection Agency (EPA), Water Sector Incident Action Checklist – Cybersecurity, https://www.epa.gov/sites/default/files/2017-11/documents/171013-incidentactionchecklist-cybersecurity_form_508c.pdf.

EPA Cybersecurity Resources for the Water Sector, https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector.

EPA Tabletop Exercise Tool for Drinking Water and Wastewater Utilities, https://ttx.epa.gov/index.html.

EPA Guidance on Improving Cybersecurity at Drinking Water and Wastewater Systems, https://www.epa.gov/system/files/documents/2024-08/epa-guidance-on-improving-cybersecurity-at-drinking-water-and-wastewater-systems-1.pdf.

EPA Cybersecurity Technical Assistance Program for the Water Sector, https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector.

Cybersecurity & Infrastructure Security Agency (CISA), Water and Wastewater Cybersecurity, https://www.cisa.gov/water.

Cybersecurity & Infrastructure Security Agency (CISA), Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

Department of Homeland Security Industrial Control Systems Resources, https://www.cisa.gov/topics/industrial-control-systems.

Department of Homeland Security, Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, https://www.cisa.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf.

National Institute of Standards and Technology (NIST), NIST Special Publication 800-61 Revision 2, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

State of Indiana, Draft Water And Wastewater Cybersecurity Plan Template, https://www.in.gov/cybersecurity/files/Water-and-Waste-Water-Treatment-CyberSecurity-Plan-Template-Final-Draft-1-3-2019.pdf.

SysAdmin, Audit, Network & Security (SANS), https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

WaterISAC, 12 Cybersecurity Fundamentals for Water and Wastewater Utilities, https://www.waterisac.org/fundamentals.