Incident Response Guide

Water and Wastewater Sector

Publication: January 2024

Cybersecurity and Infrastructure Security Agency
Federal Bureau of Investigation
Environmental Protection Agency

Executive Summary

Cyber threat actors are aware of—and deliberately target—single points of failure. A compromise or failure of a Water and Wastewater (WWS) Sector organization could cause cascading impacts throughout the Sector and other critical infrastructure sectors.

There are many aspects of the large and complex WWS Sector that pose challenges to raising cyber resilience sector wide:

- Governance and regulation involve a mix of federal and state, local, tribal, and territorial authorities.
- Cybersecurity maturity levels across the sector are disparate.
- Often, WWS Sector utilities must prioritize limited resources toward the functionality of their water systems over cybersecurity.
- Universal solutions to cyber challenges in a diverse, target-rich, and resource-poor environment are unfeasible.

To provide meaningful cybersecurity support to the WWS Sector that can help with these challenges, CISA—in conjunction with the Environmental Protection Agency (EPA) and the Federal Bureau of Investigation (FBI), as well as the federal government and WWS Sector partners listed in this guide's acknowledgement section—has created this joint Incident Response Guide (IRG) for the WWS Sector.

The unique value[1] of this joint IRG is that it provides WWS Sector owners and operators information about the federal roles, resources, and responsibilities for each stage of the cyber incident response (IR) lifecycle. Sector owners and operators can use this information to augment their respective IR plans and procedures. By empowering individual WWS Sector utilities, the authors of this guide—CISA, FBI, EPA, and the acknowledged federal government and WWS Sector partners—aim to drive improvements to cyber resilience and incident response across the WWS Sector.

[1] Multiple resources exist to guide incident response (IR) planning, e.g., National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2 (NIST SP 800-61).

Acknowledgments

In addition to the co-sealers—the Environmental Protection Agency and the Federal Bureau of Investigation—the Department of Homeland Security's Office of Intelligence and Analysis (DHS I&A) contributed to this IRG.

In addition, the following individuals and organizations contributed to this IRG: AlexRenew, American Water, Association of State Drinking Water Administrators (ASDWA), Center on Cyber and Technology Innovation (CCTI), City of Dover, Cyber Readiness Institute (CRI), DC Water, Dragos, East Bay Municipal Utility District, EMA Inc., Google/Mandiant, International Society of Automation (ISA), Maine DHHS CDC Drinking Water Program, Microsoft, New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), Platte Canyon Water & Sanitation District, San Francisco Public Utilities Commission (SFPUC), Schneider Electric, Tenable, Tetra Tech, Trinity River Authority of Texas, Water Environment Federation, WaterISAC, West Yost Inc., Xylem, and individuals from the American Water Works Association (AWWA).

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA, FBI, and EPA do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoritism by CISA, FBI, or EPA.

Table of Contents

Purpose

As the national coordinator for critical infrastructure security and resilience, CISA created this incident response guide (IRG)—along with the Federal Bureau of Investigation (FBI), the Environmental Protection Agency (EPA), and the federal, nonprofit, and private sector partners acknowledged above—to provide information about how Water and Wastewater Systems Sector (hereafter simplified as "WWS") utilities can work with federal partners during each stage of the cyber incident lifecycle.[2] This IRG advises WWS utilities on both the suitability and means of collaboration with specific federal entities for each lifecycle stage. Utilities can use this IRG to augment their IR planning and collaborate with federal partners and the WWS before, during, and following a cyber incident. **Note:** Water utilities with the means and capability to participate in a broader collective IR process during a cyber incident should see Annex I: A More Advanced Collective Response.

Scope

This guide provides information on the potential IR roles, resources, and responsibilities of specific federal government entities in supporting WWS entities, during each stage of the cyber incident lifecycle. This guide also serves to contextualize the importance, and potential impact of, a WWS cyber incident to national security.

This guide does not:

- Mandate action.
- Provide exhaustive cyber best practices.
- Establish requirements.
- Recommend technical configurations.
- Share cyber threat information.
- Endorse vendors, vendor products, or vendor services.
- Conflict, replace, or supersede existing regulatory or other legal requirements.

Audience

CISA, EPA, FBI, and partners have tailored this guide for U.S. WWS utility owners and operators, specifically, WWS utility personnel dedicated to cyber incident planning and response. These personnel should reference this guide for information on federal roles, responsibilities, and resources related to cyber incident response. Familiarity with this information will better prepare WWS utilities to respond to—and recover from—a cyber incident. **Note:** Technical expertise is not required to effectively use this guide.

---

[2] As defined by NIST SP 800-61: SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

Threat Background

Malicious cyber actors have varying goals and capabilities, which can result in a wide range of threat activity. The dependency that many U.S. critical infrastructure sectors—including Energy and Healthcare and Public Health—have on the WWS makes the Sector a target for cyber threat actors. In targeting U.S. WWS critical infrastructure, malicious cyber actors conduct activities in alignment with their overarching goals, which may be financially and/or politically motivated. In recent years, various malicious cyber incidents have impacted WWS including, but not limited to, unauthorized access, and ransomware.[3]

Cyber threat actors frequently use ransomware against WWS utilities. On internet-facing operational technology (OT) networks, ransomware can quickly propagate to affect operations. For example, in July 2021, criminal cyber actors used the ransomware ZuCaNo, via remote access, to compromise a supervisory control and data acquisition (SCADA) computer on the OT network of a Maine-based WWS utility. This incident caused the utility to revert to manual control of critical processes. Additionally, in August 2021, malicious cyber actors used Ghost variant ransomware against a California-based WWS utility. The ransomware variant resided in the system for about a month before discovery when three SCADA servers displayed a ransomware message.[4]

Nation-state cyber actors also have demonstrated an intent to target U.S. WWS utilities. According to joint Cybersecurity Advisory IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities,[5] in November 2023, the cyber actor group "CyberAv3ngers," which is affiliated with Iranian Government's Islamic Revolutionary Guard Corps (IRGC), targeted and compromised Israeli-made Unitronics Vision Series programmable logic controllers (PLCs) used at U.S. WWS utilities. The cyber actors likely accessed the affected device by exploiting cybersecurity weaknesses, including poor password security and exposure to the internet.

---

[3] FBI, CISA, EPA, NSA. "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." Joint Cybersecurity Advisory. Oct. 25, 2021. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a.

[4] Ibid.

[5] FBI, CISA, NSA, EPA, INCD. "Cybersecurity Advisory IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities." Joint Cybersecurity Advisory. Dec. 1, 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

Collective Response

1. Key Federal Partners

Dozens of federal entities work to secure cyberspace. For the purposes of this guide, however, WWS utilities can narrow their focus to federal partners with direct cybersecurity equity in the WWS: CISA, EPA, FBI, the Office of the Director of National Intelligence (ODNI), and the DHS Office of Intelligence and Analysis (I&A).

CISA is the operational lead for federal cybersecurity, the national coordinator for critical infrastructure security and resilience, and serves as the lead federal agency for asset response. CISA works closely with:

- EPA, which is the WWS's Sector Risk Management Agency.
- FBI, which is the federal lead for threat response, counterterrorism and counterintelligence, and federal law enforcement.
- ODNI, which is the intelligence lead for threat awareness and analysis.
- DHS I&A, which is the lead for delivering intelligence to state, local, tribal, and territorial (SLTT) and private sector partners.

Each of these federal entities performs distinct and critical roles in securing the WWS, leveraging their respective authorities and executive policy.

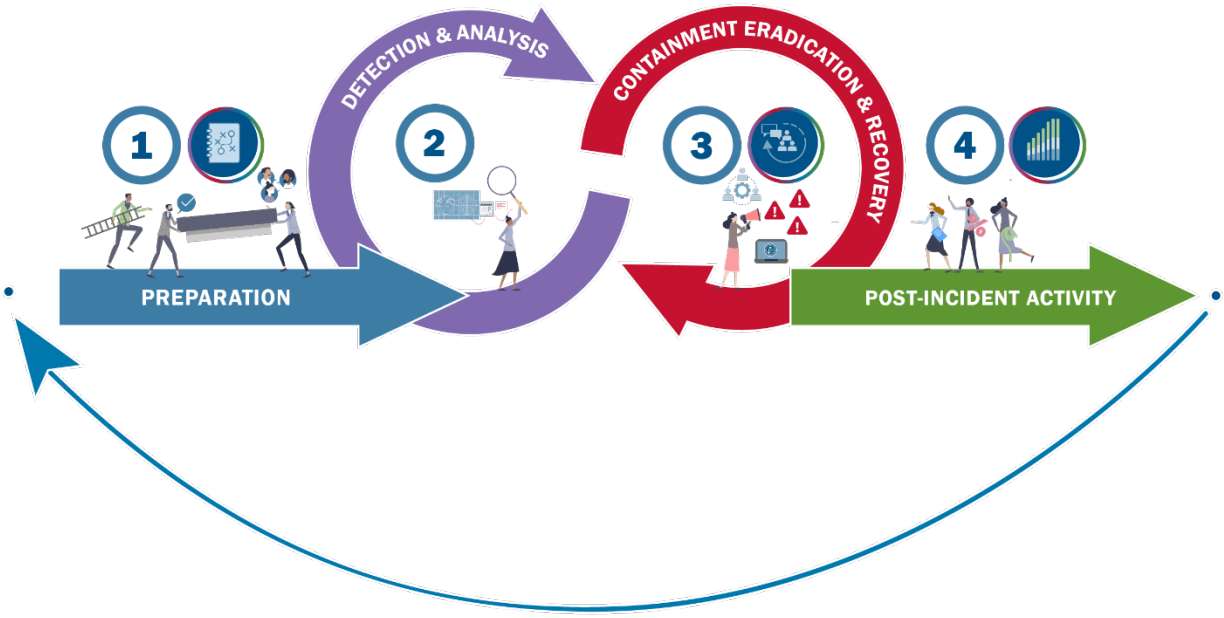
As WWS utilities navigate this guide, they should consider the role(s) these federal partners may have in individual IR plans and the resources, tools, and services available from these partners.

1.1. Information Sharing

Utilities should keep in mind that specific information they can provide to federal partners about a cyber incident could be invaluable. Bi-directional information sharing drives the collective federal response and supports the provision of critical support to affected entities. In incidents involving more than one entity, bi-directional information sharing can enable the federal government to build and share a complete picture.

2. Incident Response Process

This section walks utilities through the IR lifecycle, identifies ways to interface with the federal-level response and highlights key measures to better posture and prepare for collaboration with federal partners. The four IR lifecycle phases, as illustrated in figure 1 and defined by NIST SP 800-61, are preparation, detection and analysis, containment, eradication and recovery, and post-incident activities.



The IR lifecycle provides organizations with a step-by-step framework for identifying and responding to a cyber incident. This IRG leverages the IR lifecycle framework, allowing WWS utilities to augment their own IR plans with information on federal roles, responsibilities, and resources.

Figure 1: Incident and Vulnerability Response Lifecycle

2.1. Preparation

Preparation, illustrated in figure 2, is the first of four stages in the IR lifecycle. Preparation may seem counterintuitive for incident response. However, preparation ensures an organization is better positioned to prevent cyber incidents and reduces both the impact and the time it takes to return to normal operations. While no two utilities have the same planning considerations, simple, prioritized steps can make preparation manageable.

IR Plan Resources

NIST SP 800-61 Computer Security Incident Handling Guide

CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks

The Environmental Protection Agency (EPA)'s Cybersecurity Incident Action Checklist

The American Water Works Association (AWWA) Water Sector Cybersecurity Risk Management Guidance

FEMA's Planning Considerations for Cyber Incidents: Guidance for Emergency Managers

Cyber Baseline Resources

CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)

CISA Cybersecurity Risk Assessments

CISA Validated Architecture Design Review (VADR) Assessments

CISA Vulnerability Scanning: vulnerability@cisa.dhs.gov

Free Cybersecurity Services & Tools

WWS Community Resources

CISA Regional Offices

Water Information Sharing Analysis Center (ISAC)

American Water Works Association (AWWA)

Water and Wastewater Agency Response Network (WARN)

Cyber Readiness Institute

Incident Command System for Industrial Control Systems (ICS4ICS)

Water Environment Federation

Figure 2: Preparation Phase

2.1.1. Building An Organizational-Level Incident Response Plan

Creating an organization-level IR plan is critical to preparing for a cyber incident and setting up a posture to engage with federal entities. No two IR plans are the same as they depend on the individual characteristics of the utility and the unique reporting requirements it has for state, local, territorial, or tribal (SLTT) authorities, cyber insurance providers, and other potential reporting obligations.[6] However, regardless of resources, size, location, reporting obligations, or ownership structure, having an individual IR plan is critical to interfacing with federal agencies during crisis.[7]

2.1.2. Raising the Cyber Baseline

Establishing a strong cybersecurity baseline that includes critical controls and safeguards found in CISA's Cyber Performance Goals (CPGs) can help an organization build a more defensible network architecture and reduce the chance of becoming an easy target of opportunity for an adversary. Improving an organization's cyber posture requires an understanding its current cybersecurity baseline. Understanding that these improvements take time and resources, CISA encourages WWS utilities to consult the CPGs to begin the journey toward strengthening their cybersecurity baseline. A strong baseline is also a critical enabler for organizations to be able to effectively detect, respond to, and recover from incidents. For example, ensuring IT/OT segmentation, having system backups, and maintaining sufficient logging practices are all recommended steps to minimizing the impacts from and maximizing an organization's ability to rapidly recover from cyber incidents.

2.1.3. Building the Water and Wastewater Sector Cyber Community

Cyber communities drive collective response. Utilities of any cyber maturity level can engage with existing groups, information streams, and local offices that enhance and raise the cybersecurity posture of the Sector. Although this engagement may cost individual utilities time and resources, it ultimately creates better conditions for collective response to a cyber incident. Thus, this guide strongly recommends utilities of all sizes investigate and integrate into their local cyber communities.[8]

2.2. Detection & Analysis

The Detection and Analysis phase, illustrated in figure 3, is the next step in the IR lifecycle. A robust response at this stage requires two critical components—(1) accurate and timely reporting and (2) rapid collective analysis—to understand the full scope and impact of a cyber incident. First, to determine whether to report an incident, the utility should do their best to validate and confirm they are experiencing a malicious cyber incident. Second, on a

[6] For more information on cyber insurance, see: Cyber Insurance | Federal Trade Commission.
[7] For more resources on building an organizational-level IR Plan, see Annex II.
[8] For suggestions on how to engage your local cyber community, please see Annex II.

case-by-case basis, the utility, at the organizational level, should follow any mandatory reporting requirements and consider optional reporting options for all confirmed incidents. Third, after confirming and reporting the incident at the organizational level, the utility should determine whether they are able to participate in state/federal-level collective analysis actions for the threat activity. **Note:** For an understanding on how collective analysis works at the federal level, please see Annex I of this guide.

[CISA's Cybersecurity Performance Goals]

[EPA's Cybersecurity Incident Action Checklist]

Organizational: Product and service vendors, insurance providers, and other third parties

SLTT: State fusion centers, emergency management offices

Federal:

EPA: Water Infrastructure and Cyber Resilience Division at watercyberta@epa.gov to voluntarily provide situational awareness

CISA: Via report@cisa.gov, calling **(888) 282-0870**, or contacting a local CISA regional office

FBI: Headquarters at www.ic3.gov or contacting a local FBI Office

CISA Technical Analysis & Support:

- **Host Forensics**
- **Network Forensics**
- **Cloud Forensics**
- **Cyber Physical Forensics (CPFS).**
- **Automated Malware Analysis**
- **Code and Media Analysis**

Figure 3: Detection & Analysis Phase

2.2.1. Validate

As a part of IR, utilities should evaluate affected systems and networks for adversary behavior.[9] Before reporting an incident, it is important to **validate** that unusual activity is not the result of common user-error related activities, like firewall misconfigurations, access control issues, etc. Here are some signs that an organization may be experiencing a malicious cyber incident:

- **Unusual System Behavior:** If a system is running slower than usual, crashing frequently, or displaying excessive pop-ups.
- **Unfamiliar Network Activity:** Network activity or traffic shows unusual or unexpected data transfers, connections to unknown IP addresses, or unauthorized access attempts.
- **Unexplained Data Loss or Modification:** Files suddenly disappear, become corrupted, or their contents are modified without authorization.
- **Security Software Alerts:** The utility's anti-malware or firewall software sends warnings.
- **Phishing Attempts:** Suspicious emails, messages, or phone calls asking for personal information or login credentials come into the utility.
- **Unusual Networks or Systems:** Unknown devices or unauthorized access points start appearing on system networks.

EPA's Cybersecurity Incident Action Checklist and CISA's Cybersecurity Performance Goals can provide further guidance to help utilities validate whether they are experiencing a cyber incident.

[9] Per CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

2.2.2. Report

Note: *The cyber incident reporting landscape is constantly evolving.*[10] *This guide is not intended to provide a comprehensive overview of all possible reporting channels. Instead, this guide is intended to supplement an organization's existing cyber incident response resources with potential illustrative examples of key reporting avenues to consider. Organizations should consult their legal counsel to identify relevant statutory, contractual, regulatory, and other legal reporting requirements that may apply at the time of the cyber incident.*

As the next phase in the IR lifecycle, the utility should review its reporting obligations and consider engaging in additional voluntary reporting and/or information sharing.

First, reporting the incident at the organizational level can provide access to support from a vendor, managed service/security service provider (MSP/MSSP), or insurance company. Second, reporting an incident at the state-level and federal-level can increase understanding of the full scope and impact of the cyber incident, especially if the incident is not isolated.

If an adversary targets multiple critical infrastructure entities, federal and state governments may not realize the full scope of an incident until it has progressed to the point of disrupting services. Federal and state government work in tandem with organizations like the WaterISAC, American Water Works Association, and Water Environment Federation (WEF) to develop a clearer picture of the Sector's threat landscape. Reporting at any level facilitates collective response.

Reporting on an ongoing or potential cyber incident could, potentially, drive numerous federal response measures. CISA may be able to determine that the vulnerable device the threat actors are exploiting in one WWS utility's OT system is commonly used across the Sector. CISA could then coordinate with the affected device's vendor so that the vendor could develop mitigation or remediation strategies and notify other customers. Additionally, cyber threat information (CTI) that a WWS utility reports may help FBI attribute malicious cyber activity to a specific nation-state or criminal advanced persistent threat (APT). Once identified, FBI could conduct law enforcement activities to deter further attacks from that APT.

Reporting can be a confusing process to navigate. Generally, there are three levels of consideration for reporting: Organization, SLTT, and federal. Table 1 provides the steps for organization- and SLTT-level reporting and table 2 provides the steps for federal-level reporting.

---

[10] Further information about U.S. federal cyber incident reporting requirements, either in effect or proposed across the U.S. federal government as of September 2023, is included in Appendix B of the DHS Report on *Harmonization of Cyber Incident Reporting to the Federal Government*, available at https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.

Table 1: Organization and SLTT Reporting Levels and Activities

Reporting Level	Activity
Organization-level reporting: There are two organizational-level reporting activities to consider.	First, if the incident involves a specific product or solution, the utility should consider immediately reporting it to the vendor's support team or **product security incident response (PSIR) team**, if available. Many vendors have PSIR teams that maintain reporting portals with email addresses and web portals to receive product incident or vulnerability information.[11]
	Second, the utility should consider reporting the incident to their designated **cyber insurance provider** to activate applicable services and protections.
SLTT-level reporting: SLTT entities have unique guidance and/or mandates for reporting cyber incidents and utilities should have a clear understanding of their state's specific requirements.	For example, the utility's state may require reporting of incidents that impact or may impact the delivery of safe drinking water to the State Primacy Agency.
	Additionally, each state has **emergency management service offices** that have a role during cyber incident response, especially if there are potential physical consequences stemming from the cyber incident.
	Finally, all states have **Fusion Centers** that track cyber incidents and individual states may have additional IR resources for utilities unable to secure third-party support.

[11] Per ISO 29147 and the FIRST.org PSIR framework vendors.

Table 2: Federal Reporting Levels and Activities

Reporting Level	Activity
Federal-level reporting:[12] As stated above, federal partners with direct cybersecurity equity in the Water and Wastewater Systems Sector are CISA, EPA, FBI, and ODNI. These are the key federal players for utilities to consider engaging, especially to enable collective IR. This guide outlines *who* to report to, *why* it is important, and *how* to do so. The sections to the right describe the potential lines of effort in terms of federal response if an incident meets the collective threshold. CISA highly encourages reporting cyber incidents to these federal entities.	**CISA** has two main methods of reporting: directly to a region or to CISA's 24/7 operational center. **CISA Regions**: A utility may report to their local CISA regional office. A regional CISA office has several functions it can perform once it confirms an incident. For example, the regional office can: • Reach out to other federal partners on behalf of the victim. • Physically go to the utility onsite to provide guidance and/or coordination. • Articulate the needs of the victim to CISA headquarters. • Coordinate with relevant state and federal fusion centers. • Assist a victim in navigating the federal response. Additionally, CISA regional offices establish personalized relationships with FBI and other federal entities when possible. See cisa.gov/regions for contact information for each region. **CISA Central:** A utility may report an incident to CISA via report@cisa.gov, or by calling (888) 282-0870. Reporting requires point of contact (POC) information from the utility, a call-back number, and a description of the incident. The advantage to reporting in this manner is that the center is operational 24/7 and ensures CISA writ large is aware of the activity.
	FBI: A utility may report an incident to **FBI Headquarters** at www.ic3.gov or by contacting a local FBI Office. The FBI encourages organizations to report, especially if the incident: • Involves significant loss in data, system availability, or control of systems. • Impacts a large number of victims. • Indicates unauthorized access to or malicious software on critical information technology systems. • Affects critical infrastructure or core government functions. • Impacts national security, economic security, or public health and safety.
	EPA: The EPA is the sector risk management agency for the WWS. Contact the **EPA Water Infrastructure and Cyber Resilience Division** at watercyberta@epa.gov to voluntarily provide situational awareness.

[12] The federal contact information in this document is up to date as of Jan. 17, 2024.

2.2.3. CISA Technical Analysis and Support

CISA and its federal partners stand ready to help organizations prepare for, respond to, and mitigate the impact of cyber incidents. On a case-by-case basis, federal agencies may be able to provide no-cost tools and services to impacted utilities. CISA may provide onsite and/or virtual technical analysis and support to an organization after receiving reporting. This support may include:

- **Tailored Guidance.** CISA may provide strategic and tactical guidance to critical infrastructure organizations affected by cybersecurity incidents through technical expertise, threat intelligence, tactical mitigations, and industry best practices. CISA tailors this guidance to the impacted organization.
- **Technical Support.** When CISA provides on-site or remote technical guidance and support, the victim will receive tailored and accessible recommendations related to findings from the analysis of the threat actor behavior and related artifacts:
    - **Host Forensics.** CISA examines a wide breadth of host systems and provides detailed analysis of endpoints and forensic artifacts (both individual and at scale) to detect adversary presence or anomalies. CISA works with affected entities to deploy technologies to facilitate engagement services, perform frequency analysis, log analysis, and other forensic analysis.
    - **Network Forensics.** CISA conducts network-level intrusion detection activities in direct support of hunt and IR engagements. CISA works with affected entities to install network-monitoring solutions to assist engagement activities, develop signatures based on network traffic to identify adversary activity, and examine network traffic at scale.
    - **Cloud Forensics.** CISA provides subject matter expertise on the security architecture, technology landscape, and incident response nexus for cloud-based technologies. CISA provides guidance on the effective utilization of cloud technologies, facilitating the utility's ability to quickly deploy incident response capabilities.
    - **Cyber Physical Forensics (CPFS).** CISA provides forensic analysis and threat hunting of environments that include industrial control systems (ICS) and/or SCADA using specially trained and experienced ICS analysts. These analysts use hunt plans tailored to specific environments and circumstances. CPFS include network traffic analysis, host analysis, and radio communications with ICS field device-level interrogation and serial protocols. CPFS analysts maintain proficiency in the general structures and methodologies found in the 16 critical infrastructure sectors to be prepared to provide expert assistance to affected ICS entities.
    - **Automated Malware Analysis.** CISA generates an automated report for submitters that provides indicators of compromise (IOCs), MITRE ATT&CK® mapping, and mitigation information.

- **Code and Media Analysis.** CISA provides in-depth malware reverse engineering analysis of malware samples. CISA provides findings via detailed Malware Analysis Reports that explain how submitted malware operated when executed and detail any associated indicators.

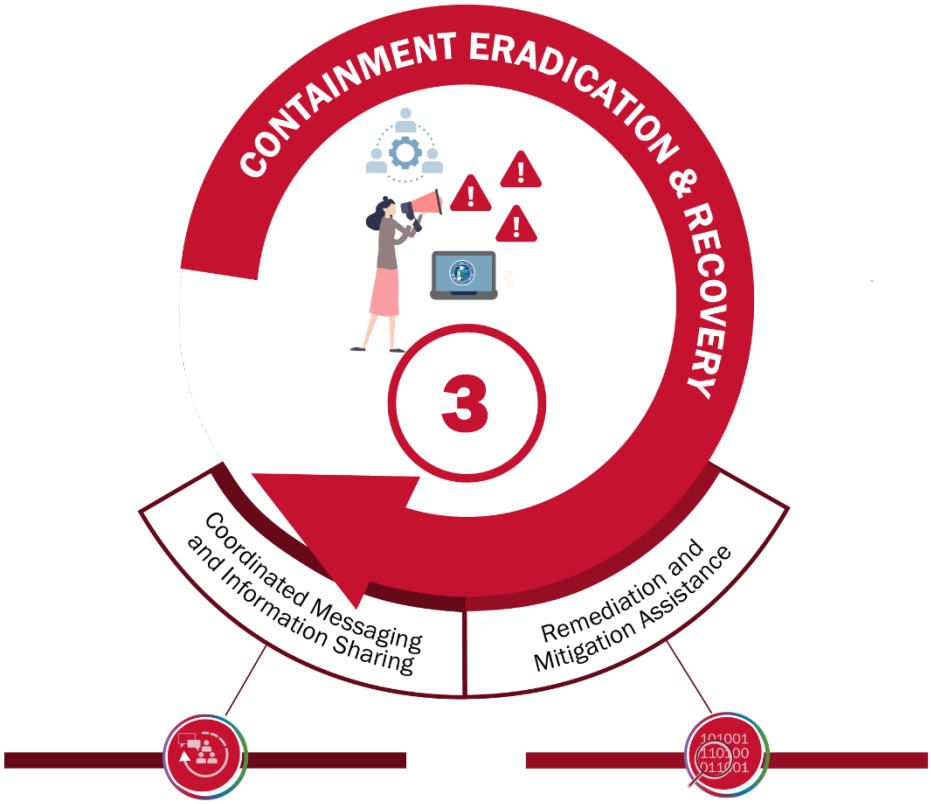
2.2.4. FBI Technical Analysis and Support

FBI has specially trained cyber squads in each of their 56 field offices, working hand-in-hand with interagency task force partners across government, to provide technical support and analysis. Like CISA, FBI deploys resources on a case-by-case basis based on reporting and prioritization mechanisms.

- The FBI's first responders to a cyber incident are the cyber special agents in the local field office. Prior to an incident, the local field office prioritizes engaging with companies, businesses, and owners and operators of critical infrastructure to build relationships and knowledge pertaining to each entity.
- When an incident occurs, the local field office manages the response and deployment of special agents and technical personnel to the site, a possible investigation, and, if applicable, the deployment of additional advanced technical capabilities like the Cyber Action Team (CAT). **Note:** When an incident occurs, the Water utility should provide the FBI: (1) the signatory authority for consent to perform investigative activities and (2) the layout of the IT and OT networks. Commonly, the FBI, at the discretion of the case team, will provide the information found as part of the investigative activities to the entity. This information may detail the findings of malicious activity or lack thereof.
- The rapid-response CAT comprises special agents and computer scientists who specialize in cyber incident response. The CAT provides investigative support and answers to critical questions that can quickly move a case forward. With advanced training in computer intrusions, forensic investigations, and malware analysis, the CAT can deploy across the country within hours to respond to major incidents. Upon activation from a case team, CAT will be onsite within 24 hours for locations in the continental United States (CONUS) and 48 hours for locations outside of the continental United States (OCONUS). See https://www.fbi.gov/news/stories/the-cyber-action-team.

2.3. Containment, Eradication, and Recovery

Containment, Eradication, and Recovery is the next step in the IR lifecycle. At the organizational level, WWS utilities will continue following their established IR Plans throughout the response process. At the collective level, meanwhile, partners will be focusing on ensuring a coordinated response throughout the containment, eradication, and recovery phase. Depending on the severity of the incident, partner focus may additionally be on coordinating technical analysis and support for impacted entities.



Continuous Information sharing among impacted stakeholders helps drive response and mitigation measures.

CISA works closely with interagency and private sector partners to share insight related to cyber incidents. CISA publishes mitigation guidance and cybersecurity advisories on their website.

EPA publishes water-specific alerts on their website, where WWS utilities can also subscribe to information outreach from the Water Infrastructure and Cyber Resilience Division (WICRD).

CISA may be able to provide impacted WWS utilities with information to help contain and eradicate unauthorized threat actors within their assets.

Remediation and mitigation assistance can include software vulnerability mitigation and advisement on advisory countermeasures and eviction.

Figure 4: Containment, Eradication, and Recovery Phase

2.3.1. Coordinated Messaging and Information Sharing

Although each cyber incident or threat is unique and requires a tailored collective response, WWS utility owners and operators should focus on the following potential activities that are likely to be a part of most responses:

- **Mitigation Guidance**: In the case of a cyber incident, CISA and other partners will develop, coordinate, and distribute relevant mitigation guidance and alerts throughout the response. These communications can include:
    - **Cybersecurity Advisories:** CISA and relevant interagency partners, e.g., FBI, develop, co-seal, and publish these advisories, which contain relevant and up-to-date technical information related to the ongoing cyber incident, including mitigations. CISA publishes these on their website.
    - **Tailored Cybersecurity Alerts:** EPA publishes water-specific alerts on their website, which also provides a sign-up form for subscriptions to general information that the Water Infrastructure and Cyber Resilience Division (WICRD) Outreach may send out.
- **Information Sharing**: Throughout the collective response, partners will continually share relevant information to support the response and defense efforts. Typical information shared with or by CISA during response efforts includes relevant adversary tactics, techniques, and procedures (TTPs), relevant indicators of compromise (IOCs), and other relevant technical data that utilities or their third-party service providers can utilize in their organizational-level response. This information will likely be shared through the communication channels established in the preparatory phases of collective response. CISA and its partners often use this information to determine the need, and content, for cybersecurity advisories.[13]

2.3.2. Remediation and Mitigation Assistance

Depending on the type of incident, CISA can provide vital information to WWS utility owners and operators on defensive measures to take to contain and eradicate unauthorized threat actors within their assets.

- **Software Vulnerability Mitigation.** CISA and other partners can develop and provide mitigations against software vulnerabilities both before and after exploitation.
- **Adversary Countermeasures and Eviction.** After exploitation and infiltration, CISA and other partners can advise on an effective course of action in countering the movement of adversaries inside WWS utility networks and assets. CISA and other

[13] For more information on information sharing with the federal government during an incident, please see Annex I.

partners may also be able to provide guidance on removing adversary methods of persistence and evicting adversary control within WWS utility networks and assets.

2.4. Post-Incident Activity

Post-Incident Activity is the last step in the IR lifecycle. At the conclusion of any cyber incident, it is important for all relevant partners to conduct a retrospective analysis of both the incident and how responders handled it. The summation of post-incident activities determines "lessons learned."

Figure 5: Post-Incident Activity

2.4.1. Evidence Retention

Evidence retention is the process of preserving data and evidence related to the incident for potential future prosecution or investigation, which is especially significant for the FBI. As a part of preparation, organizations should have a well-defined process for preserving data and evidence related to cyber incidents. This process should include clear guidelines for data collection, storage, and access. CISA and its interagency partners strongly urge utilities to implement this process in their planning. Regional CISA or FBI offices can provide guidance on data retention.

2.4.2. Using Collected Incident Data

On a voluntary basis, CISA and its interagency partners collect data from impacted organizations, anonymize it, and share the anonymized data broadly to support cyber defenders across the critical infrastructure space. This data may include relevant TTP, IOCs, and other technical data that may support collective defense.

2.4.3. Lessons Learned

CISA and its partners will collect lessons learned from the response effort. A lessons-learned analysis enables all partners to review the effectiveness and efficiency of incident handling. Often, this process can be as simple as a meeting of all the responders to review the incident chronologically. Assessing information gleaned through evidence retention can drive practical, non-technical solutions. For example, well maintained logs from the incident can reveal the number of hours personnel spent performing specific tasks, which may inform how an organization handles future incidents. Consolidating lessons learned into a formal report is an effective way to memorialize key factors, educate new personnel, and raise situational awareness across an organization.

Annex I: A More Advanced Collective Response

The Water and Wastewater Sector is large and complex. Cybersecurity maturity levels across the sector are disparate. Often, WWS utilities must prioritize limited resources toward the functionality of their water systems over cybersecurity. Therefore, CISA does not expect utilities to participate in collective action to respond to a cyber incident beyond managing their own organizational response. However, to the extent possible, CISA welcomes and encourages participation in its collective response efforts from relevant partners across the sector. In this case, CISA welcomes participation also from WWS utilities who are not the specific victims of the incident. The following Annex describes the coordination activities utilities may experience should they opt into collective activities.

A. Collective Analysis

As the national coordinator for critical infrastructure security and resilience, CISA participates in the federal review and triage of reported sector incidents, conducting collective analysis to determine the incident's size and scope. CISA coordinates with federal partners to discover the full impact and any cascading or cross-cutting impacts across other critical infrastructure sectors. As appropriate, CISA engages relevant external partners to gather additional information, evaluate the severity of the incident(s), and build common situational awareness.

Collective evaluation of a cyber incident has two purposes. First, it prompts information sharing that will either inform mitigation or remediation activities. Second, it helps partners determine if collective action is warranted.

Based on results from the evaluation period, relevant partners (federal agencies, SLTT authorities, MSPs/MSSPs, ICS vendors, etc.) will work together on next steps for mitigation or remediation. Partners should rely on their own IR plans and policies to inform specific mitigation or remediation activities but may have opportunities to align and coordinate those activities moving forward. Coordination steps CISA may take at this stage include:

- **Communication Channels.** CISA may stand up real-time chat (e.g., Slack) dedicated for a specific incident and include relevant technical, legal, policy, and communications points of contact from partner organizations.
- **Rules of Engagement.** CISA and its partners will collectively determine the frequency of stakeholder meetings and means of communication (primary, alternate, and emergency).
- **Collective Criteria.** CISA and its partners will strive to establish success criteria to determine when operations can return to a pre-incident cadence of operations.

To invite participation in collective response activities, CISA may contact a utility proactively, for example directly, through another federal agency, or through an SLTT, ISAC or association partner. Any participation in collective response led by CISA is conducted on a strictly voluntary basis.

B. Collective Response

After the initial collective analysis is complete, CISA and its partners may decide to continually coordinate and collaborate on a response. Below are some of the ways this collaboration may manifest:

- **Snap and Regular Incident-Specific Meetings.** CISA may host a snap-meeting for relevant partners—including relevant WWS entities—with the purpose of 1) providing baseline information about the incident(s) for partners and 2) soliciting updates or recommendations from partners on next steps.
- **Technical Coordination.** CISA and its partners may coordinate on providing technical services to victims, depending on the severity of the incident(s).
- **External Communications Coordination.** CISA and its partners may coordinate on external messaging as appropriate. Partners typically support the development, distribution, or amplification of public mitigation guidance, alerts, and advisories to affected parties.
- **Continued Information Sharing.** Effective collective IR depends on close operational collaboration and technical information sharing between relevant partners. This information sharing usually occurs via previously established communications channels (as described in the "Collective Analysis" section), direct technical exchanges between organizations, or through automated technical information sharing processes. The type of information continually shared usually includes technical details (e.g., IOCs, TTPs) and mitigation strategies (e.g., physical countermeasures, enhanced logging).

C. Post-Incident Collective Activities

Typically, CISA will conduct a review following an incident to collect observations, lessons learned, best practices, and areas for improvement related to CISA planning and operations associated with the cyber incident.

- **Lessons Learned Assessment.** Prior to demobilization, CISA may solicit input from all parties who were involved in the process to assess the response. This is an opportunity for partners to provide feedback on the response process, as well as retrospectively consider highlights of the collaboration, challenges of the collaboration, and reflection on bandwidth considerations and further preparation activities that may improve collaboration with the relevant operational community in the future.

Annex II: Preparation Resources

The below list provides resources for actioning the recommendations in the *2.1: Preparation* section of this document.

A. Building an Organizational-Level IR Plan:

- NIST SP 800-61 Computer Security Incident Handling Guide: This guide is foundational for creating organizational-level IR plans. The guide is universal and applicable for any organization, agnostic of sector. Many other IR guides map to or reference this publication.
- The Environmental Protection Agency (EPA)'s Cybersecurity Incident Action Checklist: The checklist covers actions to take to **prepare** for an incident, to **respond** to an incident, and to **recover** from an incident.
- The American Water Works Association (AWWA) Water Sector Cybersecurity Risk Management Guidance: This guidance provides a voluntary and sector-specific approach for adopting the NIST Cybersecurity Framework.
- CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks: Tailored to federal civilian executive branch (FCEB) agencies, these playbooks provide a standard set of procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents and vulnerabilities affecting FCEB systems, data, and networks. Though the playbooks are for the FCEB, WWS utilities may find them helpful in building their own plans.
- The Federal Emergency Management Agency (FEMA)'s National Incident Management System (NIMS): This system guides all levels of government, nongovernmental organizations, and the private sector on how to work together to prevent, protect against, mitigate, respond to and recover from incidents. Although the referenced incidents are *not* restricted to cyber incidents, the guide provides critical insights to consider when building individual IR plans.
    - Planning Considerations for Cyber Incidents: Guidance for Emergency Managers: FEMA developed this guide in coordination with CISA to help SLTT emergency management personnel collaboratively prepare for a cyber incident and support the development of a cyber IR plan or annex. While focused on the roles and responsibilities that government emergency managers may have, emergency managers in academia, nonprofits, or the private sector should also find the concepts helpful.
    - The Incident Command System (ICS) is a management system designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. The ICS

Resource Center (fema.gov) includes training, job aids, and reference materials.

  - For more help understanding and implementing FEMA's ICS, reference the AWWA informational series Making ICS Easy for Water and Wastewater Systems of Any Size .

- **Vendor-Specific Resources**: Product vendors that utilities work with may have additional resources and recommendations for organizational-level IR plans. For example, vendors may recommend establishing a collection management framework: A key component to accelerating incident investigation and response is understanding the key information utilities need to collect and how long, and where, to store it. Establishing a collection management framework helps an organization quickly translate suspicious activity into a set of hypotheses and know what data is available to help tell the difference between a cyber incident and a benign event. A product vendor should be able to instruct on what data is logged and the method of accessing those logs.

B. Resources to Raise the Cyber Baseline:

There are a variety of resources aimed at understanding an organization's cyber baseline and improving cyber hygiene:

- **Cybersecurity Performance Goals (CPGs):** CISA's CPGs are a subset of voluntary cybersecurity practices to help small- and medium-sized organizations kickstart their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes.

- **15 Cybersecurity Fundamentals for Water and Wastewater Utilities:** WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities guide contains best practices, grouped into 15 main categories, that water and wastewater systems can implement to reduce security risks to their IT and OT systems. Each recommendation contains links to corresponding technical resources, providing information for a dive deep into each topic.

- **Conducting a Cybersecurity Risk Assessment:** Conducting a risk assessment helps an organization understand the cyber risks to their operations, organizational assets, and individuals. CISA Regional Offices may be able to help set up risk assessments for WWS utilities.

- **Conduct a Validated Architecture Design Review (VADR) Assessment:** A VADR is an assessment based on federal and industry standards, guidelines, and best practices. Assessments can be conducted on IT or OT infrastructures (ICS-SCADA). Assessments focus on 1) Evaluation of Architecture, 2) Analysis of Network Traffic, and 3) Systems Log Review and Analysis. CISA Regional Offices may be able to help set up VADRs for WWS utilities.

- **Vulnerability Scanning:** CISA uses automated tools to conduct vulnerability scanning on external networks. These tools look for vulnerabilities and weak configurations that adversaries could use to conduct malicious cyber activity. Scanning provides an external, non-intrusive review of internet-accessible systems. The scanning does not reach the organization's private network and cannot make any changes. CISA sends participants weekly reports with information on known vulnerabilities found on internet-accessible assets, week-to-week comparisons, and recommended mitigations.

    - Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Vulnerability Scanning Services." Include the name of your utility, a point of contact with an email address, and the physical address of your utility's headquarters.

    CISA will reply with a Service Request Form and Vulnerability Scanning Acceptance Letter to obtain the necessary information about your utility and your authorization to scan your public networks.

- **CISA Free Tools and Services:** CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community.[14]

- **NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security:** This document provides guidance on how to secure OT while addressing their unique performance, reliability, and safety requirements. Includes an overview of OT and typical system topologies, identifies common threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

C. Building the Water Cyber Community

Operational communities drive collective response. Utilities of any cyber maturity level can engage with existing groups, information streams, and local offices to raise the cybersecurity posture of the Water Sector. Engagement may cost individual utilities time and resources but ultimately creates better conditions for collective response to a cyber incident.

- **Engage with your Water Information Sharing Analysis Center (ISAC):** Generally, most critical sectors have individual ISACs that serve as a clearinghouse for government and private information that helps members identify risks and prepare for emergencies. WaterISAC is the ISAC for the Water Sector. Join WaterISAC through their website.

[14] See CISA's Free Cybersecurity Services and Tools | CISA page.

- **Get to Know your State, Local, Tribal, and Territorial (SLTT) Offices:** SLTT governments are key partners to help prepare for, and respond to, a cyber incident. In addition to providing cybersecurity resources and guidance, SLTT authorities can provide information on any laws and regulations that may inform IR planning. For example, data breach notification requirements vary by state. The compromise of personally identifiable information (PII), such as customer billing addresses, may require different actions from the utility depending on the state of residence of the affected customers.
- **Get to Know Federal Regional Offices:** Utilities can access the breadth of CISA's resilience building, risk mitigation, and IR capabilities through 10 regional offices, which understand the planning considerations unique to specific communities, states, and regions. Consider scheduling an Assist Visit through the appropriate regional office to explore opportunities for improving information sharing with government partners, identifying vulnerabilities, and driving down risk.
- **Explore Nonprofit Associations:** There is a broad community of non-profit organizations available to support WWS utility IR planning, preparedness, and response. The Cyber Readiness Institute (CRI), American Water Works Association (AWWA), and the Incident Command System for Industrial Control Systems (ICS4ICS) are examples of such collaborative opportunities. In addition to providing direct resources and training, engaging with non-profit partners builds relationships and drives cooperation across the Sector.
- **Join Your State WARN or other Mutual Aid organizations:** A Water and Wastewater Agency Response Network (WARN) is a network of utilities helping other utilities to respond to, and recover from, emergencies. Participation in a WARN allows utilities that have sustained, or anticipate, damages from natural or human-caused incidents to provide and receive emergency aid and assistance in the form of personnel, equipment, materials, and other associated services as necessary from other WWS utilities.
- **Understand how to engage vendors' product security incident response (PSIR) capabilities:** The OT in water and wastewater systems often comprises products from multiple vendors of industrial control systems. In turn, these vendors typically have Product Security Incident Response Teams (PSIRT) in place for handling responses to vulnerability reports and incidents specific to those products. Understanding and even rehearsing vendor PSIR processes can augment utility IR planning (e.g., how does a vendor notify customers of a vulnerability associated with a specific device?).