WATER ISAC

12 Cybersecurity Fundamentals for Water and Wastewater Utilities

Recommended Practices to Reduce Exploitable Weaknesses and Consequences of Attacks

DECEMBER 2024

Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures
Fundamental 11 | Secure the Supply Chain
Fundamental 12 | Participate in Information Sharing

waterisac.org/fundamentals

10 Develop and Enforce Cybersecurity Policies and Procedures (Governance)

WHY THIS IS IMPORTANT: Documented cybersecurity policies and procedures are necessary for organizations to protect assets and mitigate risks. Policies provide a framework for identifying potential vulnerabilities, outlining security measures, and managing threats. Procedures should be detailed, step-by-step instructions that describe how to carry out policies by addressing the "who," "when," and "how" of policy implementation.

Developing policies and procedures can be one of the most straightforward and yet challenging fundamentals to implement. Regardless of difficulty, it is essential to develop and enforce clear and actionable cybersecurity policies and procedures for all OT and IT systems. Policies and procedures should plainly define an organization's cybersecurity expectations and instructions on compliance for each subject area.

Once formalized, policies and procedures can only be effectively operationalized across an organization through dissemination, communication, education, and enforcement. Distributing and communicating cybersecurity policies throughout the entire organization is vital. All staff must be made aware of their responsibility to uphold policy and follow procedures, as well as the consequences of any violation.

Policies and procedures fall under the overarching framework of governance. Policies support governance objectives as high-level principles that describe the "what" and "why" of organizational actions and guide behavior. Governance is important. So much so that it was incorporated into the NIST Cybersecurity Framework (CSF) 2.0 released in February 2024. According to NIST, the CSF's governance component emphasizes that cybersecurity is a major source of enterprise risk that senior leaders should consider alongside others such as finance and reputation.[1]

Rinse, Repeat, and Audit

Governance is a continuous endeavor. Organizational environments and cybersecurity

requirements are dynamic. Like all recommendations in these fundamentals, policies and procedures are not one-and-done. These documents need to be reviewed regularly, updated when necessary, and subsequently communicated as changes are made. Furthermore, policies and procedures must be regularly audited for accuracy, understanding, efficiency, and compliance among staff.

Policy Examples

The whole of this document, WaterISAC's *12 Cybersecurity Fundamentals for Water and Wastewater Utilities* include practical subject areas (the fundamentals) to inform the development of cybersecurity policies and procedures for your utility. Specific policy examples could include (but are not limited to) data breach response,

1 https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

acceptable use of equipment and computing systems (including email), remote access, artificial intelligence, and disaster recovery.

The SANS Institute provides a free set of templates covering important security requirements that can be customized to jump-start your policy development and implementation. At the time of this writing, SANS[2] has 64 policy templates across subject areas of email security, password creation and protection, artificial intelligence, server security, network security, incident handling, and more.

RECOMMENDED RESOURCES

How Do Cybersecurity Policies and Procedures Protect Against Cyberattacks? | Trellix

Security Policy Templates | SANS Institute

OT/ICS policy templates that will save you time, labor, and project risk | Langner

Simple Cyber Governance Program (SCGP) | Langner *(licensing is required for full access, but asset owners are able to request an evaluation copy)*

Kansas Unveils Cyber Program to Safeguard Water Systems | government technology

State Cybersecurity Governance Case Studies CROSS SITE REPORT (December 2017) | CISA

2 **https://www.sans.org/information-security-policy/**

11 Secure the Supply Chain (service providers, integrators, and other "trusted" third parties)

WHY THIS IS IMPORTANT: Engaging with third-party vendors expands a utility's attack surface whereby cyber threats can infiltrate a utility through its supply chain. Likewise, as third parties often have access to sensitive data/information, this necessitates regular assessments of third-party security postures. A supply chain or third-party risk management strategy helps identify and mitigate potential threats and contributes to maintaining operational integrity by reducing the risk of disruption to critical (operational or business) processes due to third parties.

Abusing Trusted Relationships

As outlined in *Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks*, integrators, contractors, consultants, vendors, and other third parties represent potential (insider) threats to an organization. Additionally, these trusted third parties also constitute vital parts of the supply chain and must be managed effectively to reduce risk to your utility. In many cases, third parties represent a risk due to the expanded attack surface of just doing business with them. However, in recent years, threat actors have been actively and increasingly leveraging these trusted relationships as a cyber attack vector due to the effectiveness and potential for large-scale compromises. Furthermore, attackers are keenly aware that smaller businesses are not always as cyber secure as the larger companies with whom they contract, thus it's not uncommon for attackers to compromise smaller organizations to gain a foothold into larger entities.

Attackers typically gain initial access by compromising the credentials or systems of a trusted partner, such as an IT service provider, managed security provider, or systems integrator. The MITRE ATT&CK® Framework describes the technique of abusing trusted relationships[1] as *adversaries that may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third-party relationship abuses an existing connection that may not be protected or receives less scrutiny than standard mechanisms of gaining access to a network.* As this attack vector continues to evolve, it's practical for organizations to prioritize technology controls that can detect and respond to these sophisticated tactics in real-time, while also fostering a culture of security awareness among employees and partners that it's okay to trust these third-party relationships, but they still must be verified.

Notable Third-Party Cyber Attacks

Target. The Target breach in 2013 is still one of the most highly referenced examples of how the compromise of a small vendor was used to infiltrate a major corporation and remains a significant cybersecurity case study highlighting the importance of robust third-party risk management. This breach was carried out due to a successful spear phishing attack against a small, less cyber-prepared vendor. Threat actors used the network credentials of a heating and ventilation company to infiltrate Target's network.

SolarWinds. Arguably the most impactful cyber incident in 2020, where over 18,000 SolarWinds customers installed a compromised Solar Winds Orion network management platform update, potentially exposing their systems to the attackers. Victims included U.S. government departments, as well as private companies like Microsoft, Intel, and Cisco. The SolarWinds attack raised concerns about supply chain vulnerabilities, potential risks associated with widely-used software platforms, and the need for improved security measures.

Log4Shell. In 2021, a critical vulnerability (CVE-2021-44228) was discovered in the widely used

1 https://attack.mitre.org/versions/v16/techniques/T1199/

open-source Java logging library, Apache Log4j 2. Log4j is widely used by enterprise applications, cloud services, Internet-of-Things, and SCADA systems across many industries including the water and wastewater sector – *Log4j is often an embedded component of Java-based ICS hardware and software*. Given common use of log4j, experts believe the full scope and impact may not be realized for years.

Unitronics Vision Series PLC with HMI. In late November 2023, a pro-Iranian hacktivist group known as CyberAv3ngers were observed targeting and compromising unsecured Israeli made Unitronics Vision Series programmable logic controllers (PLCs) across multiple water and wastewater utilities across the U.S. The actors gained access to the components using the well-known default credentials ("1111") of the Unitronics devices. See *Fundamental 6 | Enforce Access Controls* for more on *Exploitation of Default Passwords on Unitronics PLCs Across the U.S. Water and Wastewater Sector by CyberAv3ngers*.

MOVEit. Also in 2023, the MOVEit Managed File Transfer application that provides secure file transfer services used by thousands of organizations and government agencies, was impacted by the CL0P ransomware group. The group was able to exploit a security flaw and deploy ransomware, leaking confidential data of approximately 77 million individuals and over 2,600 companies globally, with U.S. companies being the most impacted (*reportedly 78% of breached companies*) including U.S. Department of Energy, Johns Hopkins, the University System of Georgia, and in Louisiana (LA), the Office of Motor Vehicles.

A Better Way to Mitigate Third Party Risks

The graphic, *Real-World Incidents | Notable Third-Party Cyber Attacks* highlights the significant challenges in managing third-party risks. While current cybersecurity measures have improved the ability to detect and mitigate cyber attacks that leverage trusted relationships, they are not foolproof. Organizations must continually adapt strategies, combining technological solutions with human vigilance and robust security policies to effectively combat this evolving threat landscape. *But what if there was another way?*

> *"As a nation, we have allowed a system where the cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day."*[2]
>
> – CISA

That statement from CISA speaks to the *Secure by Design*[3] effort currently underway to significantly reduce the risk from third parties. As CISA suggests, the balance of cybersecurity risk should be shifted. While, asset owners cannot ultimately be absolved from cybersecurity risk, it's not fair to put the total cost on customers for securing products they use or for manufacturers to charge more to deliver a secure product. Until the technology ecosystem takes more responsibility for manufacturing and delivering secure products and services out of the box, all organizations still have a responsibility to manage third party risk. However, in the meantime, we all have a role to play in hopes of hastening the shift in burden – asset owners can make strides by demanding secure by design and secure by default products and services.

Demand Secure by Design and Secure by Default

Each utility is responsible for its own cybersecurity, but we aren't all experts. It's impractical for asset owners and operators to understand everything there is to know about the devices and software used to build our infrastructure – *all the features, functions, secure configurations, vulnerabilities, etc.* – especially for smaller or less resourced utilities. Therefore, we all must work with manufacturers, suppliers, and integrators to demand *secure by design* products and *secure by default* configurations for the systems we use.

2 https://www.cisa.gov/securebydesign
3 Ibid.

You can help prevent insecure products
Water and wastewater utilities are encouraged to proliferate the *Secure by Design* effort. When shopping for products and services, consider the 256 (at the time of this writing) organizations that have taken the *Secure by Design Pledge*.[4] If working with one of the pledge signers is not possible, do your part to drive a secure technology ecosystem through *Secure by Demand*.[5] The *Secure by Design* guidance includes information that can **help customer organizations demand security when in procurement discussions, including questions**[6] **that customers should ask** hardware and software manufacturers, integrators, service providers, resellers, etc. to understand the extent to which the products and services have been designed with security in mind.

Until We Achieve Secure by Design and Default

Until products are secure by design, robust third-party risk management is still necessary to identify, assess, and control risks that arise from interactions with external parties.

NIST Cybersecurity Framework (CSF) 2.0 | Cybersecurity Supply Chain Risk Management (C-SCRM)
In recognizing the compound and complex nature of cybersecurity risk from third parties, as part of the new Govern (GV) function, the NIST CSF 2.0 has placed added emphasis on supply chain risk management (SCRM). Cybersecurity SCRM (C-SCRM) is a systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures.[7] Utilities are encouraged to use the CSF 2.0 to foster cybersecurity risk oversight and communications with stakeholders across supply chains.

RESOURCE | NIST CSF 2.0 | Cybersecurity Supply Chain Risk Management (GV.SC):

Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders[8]

- **GV.SC-01:** A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders
- **GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally
- **GV.SC-03:** Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes
- **GV.SC-04:** Suppliers are known and prioritized by criticality
- **GV.SC-05:** Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties
- **GV.SC-06:** Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships
- **GV.SC-07:** The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship
- **GV.SC-08:** Relevant suppliers and other third parties are included in incident planning, response, and recovery activities
- **GV.SC-09:** Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle
- **GV.SC-10:** Cybersecurity supply chain risk management plans include provisions for activities that occur after a the conclusion of a partnership or service agreement

4 https://www.cisa.gov/securebydesign/pledge
5 https://www.cisa.gov/resources-tools/resources/secure-demand-guide
6 https://www.cisa.gov/sites/default/files/2024-08/SecureByDemandGuide_080624_508c.pdf
7 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

It's important for utilities to effectively manage third party risk by conducting comprehensive risk assessments of third-party vendors and implementing strong contractual obligations that include specific security requirements. Relevant CISA *Cross-Sector Cybersecurity Performance Goals (CPGs)*[8] to manage third-part risk include:

CPG | 1.G Supply Chain Incident Reporting[9]

Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents within a risk-informed time frame, as determined by the organization.

CPG | 1.H Supply Chain Vulnerability Disclosure[10]

Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk informed time frame, as determined by the organization.

CPG | 1.I Vendor/Supplier Cybersecurity Requirements[11]

Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.

Beyond the Inherent Risk Posed from Third Parties

Beyond the inherent risk posed to organizations via third parties from the use of hardware, software, etc., threat actors also usurp trusted relationships that exist due to human interactions. Attackers use social engineering methods such as various phishing techniques to exploit human vulnerabilities to gain unauthorized access to systems, finances, and sensitive information. According to member reports captured in the *WaterISAC Quarterly Water Sector Incident Summaries* – TLP:AMBER reports offering a look at incidents impacting water and wastewater utilities during a specific quarter – most member reported incidents consistently highlight phishing attacks, particularly those involving impersonation of a trusted entity, such as business email compromise (BEC) and vendor email compromise (VEC). These phishing attacks often include a range of deceptive themes like invoice fraud.

Notable WaterISAC Member Reports of Third-Party Incidents

Incidents at trusted third-party vendors had impacts on multiple members.

There was a report of **QR code phishing** involving impersonation of a trusted vendor and several other reports of **vendor impersonation** attempts and **indirect impacts** on a utility from ransomware incidents at a vendor. One of the more notable incidents involved the compromise of a **third-party paper check processing vendor** which led to some of the utility's customers having images of their checks posted on the dark web.

Insufficient employee awareness about third-party risk management can increase the risk to these types of attacks. As such, employee awareness (*Fundamental 3 | Create a Cyber Secure Culture and Protect from Insider Risks*) cannot be overstated in helping curb threats from third parties. Additionally, it is crucial to establish policies and procedures (*Fundamental 10 | Develop and Enforce Cybersecurity Policies and Procedures*) to verify communications from vendors. Internal staff must be empowered by leadership to be extra vigilant and not blindly trust requests that appear to come from a trusted partner. Staff that manage vendor relationships, especially financial aspects, should be immersed in advanced training regarding these threat actor tactics.

8 https://www.cisa.gov/cybersecurity-performance-goals
9 https://www.cisa.gov/cybersecurity-performance-goals-cpgs#SupplyChainIncidentReporting1G
10 https://www.cisa.gov/cybersecurity-performance-goals-cpgs#SupplyChainVulnerabilityDisclosure1H
11 https://www.cisa.gov/cybersecurity-performance-goals-cpgs#VendorSupplierCybersecurityRequirements1I

Small Systems Guidance

Managing third-party relationships can be particularly challenging for small utilities due to limited resources and lack of experience. It's not uncommon for small organizations to struggle with things like:

- Conducting due diligence and getting third parties to share sensitive information about their security practices. (CISA's *Secure by Design* guidance contains questions that utilities can use as a starting point to assess a third party's security practices).
- Effectively identifying and documenting all third-party relationships.
- Creating and enforcing robust vendor risk management policies.
- Developing and maintaining an effective incident response plan for third-party-related security incidents.

RESOURCE | Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem[12]

Below are questions that utilities can use as a starting point *for assessing a manufacturer's approach to product security or when in procurement discussions with third party integrators, resellers, or service providers.*

- Has the manufacturer taken CISA's Secure by Design Pledge? What progress reports has the manufacturer published in line with its commitments to the pledge?
- How does the manufacturer make it simple for customers to install security patches? Does it offer support for security patches on a widespread basis and enable functionality for automatic updates?
- Does the manufacturer support integrating standards-based single sign-on (SSO) for customers at no additional cost? If the software manufacturer manages authentication, does it enable multi-factor authentication (MFA) or other phishing-resistant forms of authentication like passkeys by default, and at no cost?
- Has the software manufacturer eliminated default passwords in its products? If not, is it working to reduce the use of default passwords across its product lines?
- What classes of vulnerability has the software manufacturer systematically addressed in their products? For those that they haven't yet addressed, do they have a roadmap showing how they plan to eliminate those classes of vulnerability?
- Does the manufacturer generate a software bill of materials (SBOM) in a standard, machine-readable format and make this available to customers? Does the SBOM enumerate all third-party dependencies, including open source software components?
- How does the software manufacturer vet the security of open source software components it incorporates and facilitate contributions back to help sustain those open source projects? Does the software manufacturer have an established process to do so, such as through an open source program office (OSPO)?
- Does the software manufacturer include accurate Common Weakness Enumeration (CWE) and Common Platform Enumeration (CPE) fields in every CVE record for the software manufacturer's products?
- Has the software manufacturer published a vulnerability disclosure policy that authorizes testing by members of the public on products offered by the software manufacturer?

To overcome these challenges, small utilities may wish to consider reaching out to larger utilities, prioritizing critical vendors, and focusing on essential risk management practices within their resource constraints.

12 https://www.cisa.gov/sites/default/files/2024-08/SecureByDemandGuide_080624_508c.pdf

RECOMMENDED RESOURCES

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (SP 800-161 Rev. 1) | NIST

NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM) | NIST

10 Questions to Ask Suppliers as Part of Third-Party Security Reviews | Dragos

Software in the Supply Chain: The Newest Insider Threat to ICS Networks | Dragos

Water Sector Cyber Resilience Briefing – You can Demand Secure by Design and Default (October 2024) | WaterISAC (members only access)

Software Bill of Materials (SBOM) | CISA

Hardware Bill of Materials (HBOM) Framework for Supply Chain Risk Management | CISA

Securing OT against Log4j; Is it really a thing? | CISA

12 Participate in Information Sharing and Collaboration Communities

WHY THIS IS IMPORTANT: No single organization can sustainably identify and address all cyber threats alone. Trusted and secure information sharing is fundamental for enhancing cybersecurity and building resilience given the rapidly changing digital landscape and the increasing sophistication of cyber threats. Information sharing allows organizations to leverage collective knowledge and experience to gain a more comprehensive understanding of potential threats and risks. By exchanging threat information and intelligence, utilities gain faster awareness of developing threats to improve proactive (rather than reactive) threat detection and response.

Participating in information sharing and collaboration communities is individually and collectively very effective. The more utilities collaborate and share with regional peers and the community at-large, the more the sector benefits. Water and wastewater utilities and other critical infrastructure sectors all face the same cyber threats. Involvement with organizations that focus on cybersecurity and resilience enables the community to learn and share knowledge and experience to help one another become more resilient.

History of Information Sharing

The importance of cyber information sharing was deemed so important that multiple federal efforts have been established to provide a framework.

Presidential Decision Directive 63 (PDD-63).[1] In May 1998, Presidential Decision Directive 63 (PDD-63) established a comprehensive framework for cyber information sharing and critical infrastructure protection in the United States. Specifically, **PDD-63 encouraged the creation of sector-specific Information Sharing and Analysis Centers (ISACs)** to facilitate information sharing between the government and private sector. Additionally, recognizing the increasing interdependence of critical infrastructures and the growing threat of cyber attacks, PDD-63 emphasized the importance of public-private partnerships and sought voluntary participation from private industry to meet common goals for protecting critical systems.

For Consideration

Key benefits of cyber information sharing:

- **Faster awareness of developing threats.** Utilities can learn about new threats as they emerge, providing more time to upgrade defenses.
- **Improved threat detection and response.** Sharing enables utilities to identify potential indicators of compromise (IoCs) and threat actor behaviors for better understanding of threats.
- **Cost reduction.** Collaborative efforts spread out the cost of cyber intelligence and security measures across multiple entities. This benefit can be especially useful for small less resourced utilities to provide awareness.
- **Enhanced collaboration.** Information sharing fosters reciprocal relationships and trust among participating organizations.
- **Proactive security measures.** Early warnings allow for more strategic use of IT, OT, and security staff, enabling a proactive rather than reactive approach.
- **Strengthened overall security.** By sharing knowledge, utilities contribute to improving security measures across industries and the internet.

1 https://www.ojp.gov/ncjrs/virtual-library/abstracts/white-paper-clinton-administrations-policy-critical-infrastructure

While PDD-63 initially introduced the concept of ISACs, Executive Order (EO) 13636[2] in 2013 further emphasized and expanded the role of information sharing in cybersecurity. **EO 13636 sought to focus on increasing the volume, timeliness, and quality of cyber threat information sharing and improve information sharing between government agencies and between government and the private sector.**

Executive Order 13691[3] | Formation of Information Sharing and Analysis Organizations (ISAOs). In 2015, Executive Order 13691 focused on enhancing cybersecurity information sharing within the private sector and between the private sector and government by promoting and encouraging the development of Information Sharing and Analysis Organizations (ISAOs). ISAOs were designed to serve any community, sector, or subsector, *not limited to critical infrastructure*, making them more inclusive than existing ISACs.

NIST *Guide to Cyber Threat Information Sharing* (SP 800-150).[4] Once again emphasizing the importance of information sharing, in 2016 NIST published *Guide to Cyber Threat Information Sharing* (SP 800-150). According to NIST, the *Guide to Cyber Threat Information Sharing* provides guidelines for establishing and participating in cyber threat information sharing relationships.

Stronger Together

WaterISAC offers a prime opportunity for utilities and other stakeholders to collaborate, share ideas, successes, incident details, and lessons learned. Other respected information sharing organizations with different strengths include the Multi-State ISAC; the Electricity ISAC; U.S. EPA's Office of Water; national, regional, and state water and wastewater associations; InfraGard; urban and regional law enforcement agencies, and intelligence fusion centers.

Share experiences. Another way to share with your peers is to develop case studies and presentations about challenges your utility has overcome. WaterISAC always welcomes content in the form of articles and webinar presentations. If you have a story to tell, or you just have a possible topic of interest to suggest, please get in touch with WaterISAC.

H2OEx. Roundtable discussions are ideal venues for peer-to-peer sharing and collaboration. In December 2024, WaterISAC hosted its first *in person discussion-based regional exercise* to a sold-out crowd in Washington D.C. (Region 3[5]). With over 70 attendees representing 21 utilities, federal partners from the EPA, FBI, and the White House Office of Cybersecurity, along with industry sponsors and sector supporters. After the success of this pilot event, plans are under way to bring similar events to additional regions[6] in 2025 and beyond. Keep an eye out for more at **https://www.waterisac.org/**, or reach out to WaterISAC at 1-866-H2O-ISAC (1-866-426-4722), or our contact form to find out more.

Conferences. Participating in association conferences is another valuable sharing/collaboration method. For example, AWWA's annual Water Infrastructure Conference (WIC) and NRWA's WaterPro offer numerous security and resilience presentations and opportunities to network with peers. Consider attending, or even presenting at WIC, WaterPro, or at events hosted by other associations.

Share Cybersecurity Incidents and Suspicious Activity with WaterISAC

Reporting suspected or confirmed incidents is extremely valuable to the sector and, in many cases, national security. Reporting incidents helps WaterISAC and government security agencies learn which threats utilities are facing. This, in turn, influences the development of knowledge, intelligence, and resources to prevent future compromises and to assist with recovery and response. Reporting OT and IT compromises also allow analysts to glean threat indicators and observed behaviors from an incident or suspicious activity. These observables can be shared to help network defenders identify and block future attacks. Potential observables include malware signatures, malicious IP addresses, suspicious URLs and files – any artifacts that can signify potentially nefarious activity.

2 https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf
3 https://obamawhitehouse.archives.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform
4 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf
5 https://www.cisa.gov/about/regions/region-3
6 https://www.cisa.gov/about/regions

Report Incidents and Suspicious Activity to WaterISAC and Authorities

"It takes a community to protect a community." That is the underlying theme of the Department of Homeland Security's **"If You See Something, Say Something®"** program. It is also the foundation of information sharing and it is what motivates WaterISAC's mission to help protect the security and resilience of our members and the water and wastewater sector at large.

WaterISAC urges utilities and others sector stakeholders to report incidents and suspicious activity to our analysts. Reporting incidents and suspicious activity helps strengthen sector resilience, because it allows WaterISAC to identify threats and vulnerabilities and to warn other members and partners. The information you share also helps WaterISAC shape products and services, including advisories, webinars, and reports that can help utilities stay safe, secure, and resilient.

Reports are Kept Confidential

WaterISAC maintains confidentiality of the information provided by submitters. If WaterISAC wishes to share your incident in an analysis or other product, we would first secure your express permission to do so, then would anonymize the information you have shared. As a private non-profit, WaterISAC is not subject to public records law, further preserving the security of your report.

In some cases, it may necessary or preferable to also report your incident or suspected incident to federal authorities, especially if you intend to seek help with an investigation or recovery. Crimes should always be reported to the appropriate authorities.

How do I make a report?
You can file reports of incidents and suspicious activity to WaterISAC in three ways:

1. Submit a confidential report at **www.waterisac.org/report-incident**.
2. Email **analyst@waterisac.org**.
3. Call our analyst desk at 866-H2O-ISAC.

What do I report?
WaterISAC seeks reports of both cyber and physical incidents, as well as suspicious activity.

Cybersecurity Incidents. Cybersecurity incidents are cyber attacks or compromises of your

DIRECTOR'S NOTE

Everyone wants to know; few are willing to share
Rarely a day goes by without seeing a headline about a disclosed/discovered cyber incident or disclosed product vulnerability. Often the impacted organizations are global brands (think Cisco, OKTA, MGM, major banks, federal/state governments, etc.) that perhaps have a duty to the world to be as transparent as possible about their experience. In the spirit of information sharing, this transparency helps all organizations know what to look for to protect their systems and infrastructure from similar attacks. These disclosures also highlight that cyber attacks can happen to anyone – regardless of organizational size, type, or cyber maturity.

But does that mean everyone has to be public about cyber attacks – absolutely not! There are other ways to share information about your cyber incident or observed suspicious activity without being so public.

Non-attributable community reporting. Non-attributable reporting is why the ISACs/ISAOs exist. **ISACs/ISAOs thrive on being able to help their sectors/communities understand the threats facing them. We do that best when we receive member reports that we anonymize and report out for the benefit of all members.** Often, less global organizations/entities are reticent to report cyber incidents for a variety of reasons. Unfortunately, too often, news of the incident ends up leaking from elsewhere – and that's unfortunate to first hear something about a sector organization's cyber incident from the mass-media news.

I encourage all water and wastewater utilities to stop keeping your cyber incidents so close to the vest *until a reporter calls*. Once you get things under control, consider making WaterISAC your next call. We're happy to assist as able, but we also value the opportunity share what you experienced for the benefit of other utilities and sector stakeholders. As shared in the ***Report Incidents and Suspicious Activity to WaterISAC and Authorities*** section, your reports are kept confidential and only shared in an anonymous fashion to help others protect their systems from similar activity.

— Jennifer Lyn Walker
Director of Infrastructure
Cyber Defense | WaterISAC

enterprise IT system or your industrial control system (ICS/OT). These events/incidents could be:

- Successful ransomware attacks or close calls.
- Successful install of malware that had or may have had an impact on the utility's ability to conduct business and/or operations.
- Phishing campaigns, including successful or attempted spear phishing of executives, executive assistants, SCADA engineers, IT administrators, financial staff, or other privileged users.
- Successful or attempted business email compromise or vendor email compromise incidents, including account takeover or impersonation of executives.
- Data thefts.
- Social engineering attempts to gather sensitive information from personnel.

Physical Security Incidents. Reportable physical security incidents include those that are intended to cause any of the following:

- Bodily harm to employees or customers.
- Public health impacts.
- Significant harm to the environment.
- Impacts to the operations of your utility.
- Financial losses to your organization of $10,000 or more (per instance.)

Specific examples of physical incidents could include:

- Intentional water supply or wastewater contamination.
- Sabotage/tampering.
- Theft.
- Assault.
- Surveillance or suspicious questioning.
- Threats.

What happens next?
Once you advise us of the incident or suspicious activity, we will follow up with you for more information. We will intentionally ask for your permission to use the information in WaterISAC reports.

> *If the answer is yes,* ***we will anonymize the information you shared by removing any details that would attribute the incident to you or your utility.*** *The information you share is stored in a protected database.*

The anonymized information will be used to inform various WaterISAC reporting – typically at a **TLP:AMBER**[7] sharing level, including (but limited to) any relevant notices/advisories, *Quarterly Water Sector Incident Summary*, or *Threat Analysis for the Water and Wastewater Sector*.

Federal and Other Reporting and Assistance Mechanisms

United States
CISA Services Portal. CISA provides a secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. You can create an account and track the progress of your issue or submit your issue anonymously for CISA's review. Other CISA contact information includes CISA Central at 1-844-Say-CISA and **SayCISA@cisa.dhs.gov**.

RESOURCE | CISA Security Advisors

Water and wastewater utilities are encouraged to maintain relationships with CISA's Security Advisors, including regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). *You may also contact WaterISAC for an introduction to CISA's Security Advisors.*

Additionally, should you require assistance, CISA offers **no-cost** Cyber Incident Response and Cyber Threat Hunting services for critical infrastructure organizations and Government entities at the Federal, State, Local, Tribal, and Territorial (FSLTT) levels.

7 https://www.first.org/tlp/

Cyber Incident Response.[8] Provides incident response, management and coordination activities for cyber incidents occurring in the critical infrastructure sectors as well as Government entities at the Federal, State, Local, Tribal, and Territorial levels.

Cyber Threat Hunting.[9] For assets related to National Critical Functions and which align to government priorities, CISA provides cyber hunting services focused on specific threat actors and their associated tactics, techniques, and procedures for the purposes of greater understanding of threat actor capabilities as well as assisting owners in securing at-risk assets.

The Protected Critical Infrastructure Information (PCII) Program enhances information sharing on the security of critical infrastructure between the public and private sectors with the government by protecting sensitive critical infrastructure information from disclosure per the Critical Infrastructure Information Act of 2002. To learn more visit ***Protected Critical Infrastructure Information (PCII) Program | CISA*** *or email* ***PCII-Assist@mail.cisa.dhs.gov****.*

Federal Bureau of Investigation (FBI). The FBI encourages victims of internet crimes to contact an **FBI field office**. Crime complaints can also be made to the bureau's Internet Crime Complaint Center (IC3) at **www.ic3.gov**.

MS-ISAC and E-ISAC. Members of the Multi-State ISAC and the Electricity ISAC should report incidents through established channels.

Fusion Centers. State or regional **Fusion Centers** are another possible reporting option. Fusion centers are effective at appropriately sharing information and have strong relationships with DHS and other organizations.

Australia
Utilities in Australia may report incidents to Australian Cyber Security Centre (ACSC) via **ReportCyber**, the Australian Government's online cybercrime reporting tool, or by calling 1300-CYBER1. If there is a threat to life or risk of harm, call 000 immediately.

Canada
Utilities in Canada may report incidents to the Canadian Centre for Cyber Security by visiting **https://www.cyber.gc.ca/en/incident-management**, calling 1-833-CYBER-88, or by emailing **contact@cyber.gc.ca**. If you believe a cyber incident is an imminent threat to life or of a criminal nature, please contact your local police services **(911)** or the RCMP. All victims are encouraged to report cybercrime activities to law enforcement.

8 https://www.cisa.gov/resources-tools/services/cyber-incident-response
9 https://www.cisa.gov/resources-tools/services/cyber-threat-hunting

RECOMMENDED RESOURCES

WaterISAC

Multi-State ISAC (MS-ISAC)

Electricity ISAC (E-ISAC)

Oil and Natural Energy ISAC (ONE-ISAC)

Drinking Water and Wastewater Resilience | U.S. EPA Office of Water

Information Sharing | CISA

InfraGard

National Fusion Center Association

Guide to Cyber Threat Information Sharing (SP 800-150) | NIST

WaterPro Conference | NRWA

Water Infrastructure Conference | AWWA

1620 I Street, NW, Suite 500
Washington, DC 20006
1-866-H2O-ISAC (1-866-426-4722)

waterisac

waterisac

waterisac.org/fundamentals