INSURANCE AGENCY
A DIVISION OF WINSTAR INSURANCE GROUP

Texas Water Cyber Solutions

Your Shield Against Data Breaches and Cyber Attacks

$1 MILLION OF COVERAGE
AS LOW AS $840
*Pricing Subject to Completed Application

Protection from Cyber Threats

In today's digital landscape, cyberattacks are a growing risk. Cyber liability insurance shields your business from data breaches, hacking, and other online threats, ensuring your operations stay secure.

Safeguard Your Client Data

Client information is one of your most valuable assets. Cyber liability insurance helps cover costs related to breaches, including notification requirements, credit monitoring, and legal fees, protecting both you and your clients.

Recover Faster After an Attack

A cyberattack can disrupt your business, but with cyber liability insurance, you'll have the support needed to restore operations quickly, from data recovery to network reconstruction and financial assistance.

Mitigate Financial Losses

The financial impact of a cyberattack can be devastating. Our cyber liability policies provide coverage for ransom demands, business interruptions, and the legal and reputational costs associated with cyber incidents.

COVERAGE HIGHLIGHTS

- Ransom Payment / Extortion
- Business Interruption
- Reputational Harm Expense
- Hardware Lock Out Costs
- Privacy & Network Security
- Regulatory Fines & Penalties
- Payment Card Costs
- And More!

Stay One Step Ahead of Cyber Threats

Reach out today to explore how Cyber Insurance can protect your business.

(800) 252-9435
info@aiainsagency.com
www.aiainsagency.com

TLP:CLEAR

Top Cyber Actions for Securing Water Systems

Overview

Water and Wastewater Systems Sector entities (herein referred to as "water systems") run operational technology (OT) and information technology (IT) systems that are too often vulnerable to cyberattacks. This fact sheet highlights the top cyber actions water systems can take today to reduce cyber risk and improve resilience to cyberattacks and provides free services, resources, and tools to support these actions, which can be taken concurrently.[1,2,3] Visit CISA's Water and Wastewater Systems Cybersecurity and EPA's Cybersecurity for the Water Sector webpages for more information and resources.

Buyer beware: Technology manufacturers make security choices that affect the quality of their software and hardware. Review CISA's Secure by Design guidance and ask your vendors how they are adopting the secure by design principles and tactics within their products to mitigate cybersecurity threats.

1. Reduce Exposure to the Public-Facing Internet

Use cyber hygiene services to reduce exposure of key assets to the public-facing internet. OT devices such as controllers and remote terminal units (RTUs) are easy targets for cyberattacks when connected to the internet.

- **Free resource**: CISA's Free Cyber Vulnerability Scanning for Water Utilities fact sheet explains the process and benefits of signing up for CISA's free vulnerability scanning program.
- **Free service:** Email vulnerability@cisa.dhs.gov with the subject line, "Requesting Cyber Hygiene Services" for CISA Cyber Hygiene Services, which proactively identify and enable timely mitigation of internet-exposed assets.

2. Conduct Regular Cybersecurity Assessments

Conduct a cybersecurity assessment on a regular basis to understand the existing vulnerabilities within OT and IT systems. Assessments enable you to identify, assess, and prioritize mitigating vulnerabilities in both OT and IT networks.

- **Free service:** EPA Cybersecurity Assessments can help assess cybersecurity posture.
- **Free resources:**
  - CISA's Cybersecurity Performance Goals (CPGs) provide a set of baseline cyber protections. A free CPG assessment can be administered by a CISA cybersecurity advisor CISA Regions) or through a self-assessment.
  - The American Water Works Association's (AWWA's) Water Sector Cybersecurity Risk Management Guidance and Risk Management Tool can help a utility examine which cybersecurity controls and practices are most applicable based on the technology applications they have implemented.
  - AWWA's Water Sector Cybersecurity Risk Management Guidance for Small Systems is a *getting started guide* that helps small, rural utilities (who serve <10,000 people) assess and implement cyber best practices.
  - The WaterISAC's 15 Cybersecurity Fundamentals for Water and Wastewater Utilities provides an overview of cybersecurity measures with resources to accompany each measure for deeper exploration.
  - The MS-ISAC's Center for Internet Security Risk Assessment Method (CIS RAM) is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Critical Security Controls (CIS Controls) cybersecurity best practices. The CIS RAM Family of Documents provides instructions, examples, templates, and exercises for conducting a cyber risk assessment.

[1] The Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA), and Federal Bureau of Investigation (FBI) jointly authored this fact sheet.
[2] Joint FBI-CISA-NSA-EPA-INCD Advisory: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. WWS Facilities
[3] Joint FBI-CISA-EPA-NSA Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems

TLP:CLEAR

3. Change Default Passwords Immediately

Require unique, strong, and complex passwords for all water systems, including connected infrastructure. Weak default or insecure passwords are easy to discover and exploit, and they may allow cyber threat actors to make changes to a water systems' operational processes. This can negatively impact public health and safety. Change default or insecure passwords and implement multifactor authentication (MFA) where possible. Focus on deploying MFA to IT infrastructure, such as email, to make it difficult for threat actors to access OT systems. Consider asking manufacturers to eliminate default passwords.

- **Free resources:** CISA's Secure our World Campaign: Use Strong Passwords and More than a Password Campaign. For additional cyber guidance, see CISA's Cyber Guidance for Small Businesses.

4. Conduct an Inventory of OT/IT Assets

Create an inventory of software and hardware assets to help understand what you need to protect. Focus initial efforts on internet-connected devices and devices where manual operations are not possible. Use monitoring to identify the devices communicating on your network.

- **Free service:** EPA's Cybersecurity Technical Assistance Program supports you in conducting an inventory.
- **Free tool:** A first step in conducting an inventory is identifying the devices on the network. CISA's Malcolm tool enables network monitoring with custom parsers designed for industrial control system (ICS)/OT protocols.

5. Develop and Exercise Cybersecurity Incident Response and Recovery Plans

Develop

Understand incident response actions, roles, responsibilities, as well as who to contact and how to report a cyber incident before one occurs to ensure readiness against potential targeting.

- **Free resources**: EPA's Cybersecurity Action Checklist and CISA's Incident Response Plan (IRP) Basics help to develop cyber incident response plans. The Joint CISA-FBI-EPA Water Incident Response Guide provides valuable information on how to work with federal response partners before, during, and after a cyber incident. **Note:** See this guide for contact information for CISA, FBI, and the EPA Water Infrastructure and Cyber Resilience Division.

Exercise

Test your incident response plan annually to ensure all operators are familiar with roles and responsibilities.

- **Free tools:** CISA Tabletop Exercise Package (CTEP) and EPA tabletop exercise (TTX) scenario tools assists critical infrastructure owners and operators in developing their own tabletop exercises to meet their specific needs.

6. Backup OT/IT Systems

Regularly backup OT/IT systems so you can recover to a known and safe state in the event of a compromise. Test backup procedures and isolate backups from network connections. Implement the NIST 3-2-1 rule: 3) Keep three copies: one primary and two backups; 2) Keep the backups on two different media types; 1) Store one copy offsite.

- **Free resources:** CISA's Cyber Essentials Toolkit Chapter 5: Your Data and NIST's Protecting Data From Ransomware and Other Data Loss Events provide guidance on backing up your systems.

7. Reduce Exposure to Vulnerabilities

Mitigate known vulnerabilities and keep all systems up to date with patches and security updates. Prioritize OT patches in accordance with CISA's Known Exploited Vulnerabilities (KEV) catalog during scheduled downtime of OT equipment; prioritize patches in IT, as applicable. CISA's Secure our World Campaign provides guidance on updating software.

8. Conduct Cybersecurity Awareness Training

Conduct cybersecurity awareness training annually, at a minimum, to help all employees understand the importance of cybersecurity and how to prevent and respond to cyberattacks.

- **Free resources:** See EPA Cybersecurity Training and CISA's free Industrial Control Systems cybersecurity virtual training to learn how to protect against cyberattacks to critical infrastructure. Also see CISA's Secure our World Campaign: Employee Phishing Training for practical steps to help your employees avoid phishing scams.

Support

If you require additional support for implementing any of these actions, contact EPA and/or your regional CISA cybersecurity advisor for assistance.

Disclaimer

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked or referenced 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 favoring by the authoring agencies.

CYBER INCIDENT
REPORTING PROCESS

WHY IS IT IMPORTANT TO REPORT CYBER INCIDENTS?

A cyber incident could jeopardize drinking water and waste water utilities by allowing access to private customer/employee information, changing chemical levels in water treatment processes, or denying access to critical systems. Cyber incidents resulting in disruptions of operational processes are of particular concern to the Federal Government. The attacker is a criminal, and reporting an incident allows individuals to look out for suspicious activity and enables them to take steps to protect themselves.

WHERE TO REPORT:

REPORT TO THE FBI FOR THREAT RESPONSE

Submit an internet crime complaint form to the FBI at *www.ic3.gov* or contact your local field office at *www.fbi.gov/contact-us/field*. The FBI will conduct the investigation.

OR

REPORT TO CISA FOR ASSET RESPONSE

Submit a computer security incident form to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System at *www.us-cert.cisa.gov/forms/report*. CISA can be contacted by phone at 888-282-0870 and by email at *Central@cisa.gov*. CISA will provide technical assets and assistance to mitigate vulnerabilities and reduce the impact of the incident.

OR

CONTACT EPA FOR CENTRALIZED RESPONSE

Please reach out to the U.S. Environmental Protection Agency (EPA) Water Infrastructure and Cyber Resilience Division (WICRD) at *WICRD-outreach@epa.gov*. EPA's WICRD will act as a centralized federal point of contact between the affected parties/stakeholders and all appropriate federal agencies incorporated in the incident response.

WHEN TO REPORT TO THE FEDERAL GOVERNMENT

Utilities are encouraged to report all cyber incidents when there is any:

- Loss of data, system availability, or control of systems;
- Impact to any number of victims;
- Detection of unauthorized access to, or malicious software present on, critical information technology systems;
- Affected critical infrastructure or core government functions; or
- Impact to national security, economic security, or public health and safety.

WHAT TO REPORT TO THE FEDERAL GOVERNMENT

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include:

- Who you are,
- Who experienced the incident,
- What sort of incident occurred,
- Details of incident impact,
- How and when the incident was initially detected,
- What response actions have already been taken, and
- Who has been notified.

Office of Water (4608T)
EPA 810-F-23-003
January 2023

Incident Action Checklist – Cybersecurity

For on-the-go convenience, the actions in this checklist are divided up into three "rip & run" sections and provide a list of activities that water and wastewater utilities can take to prepare for, respond to and recover from a cyber incident. You can also populate the "My Contacts" section with critical information that your utility may need during an incident.

Cyber Incidents and Water Utilities

Cyberspace and its underlying infrastructure are vulnerable to a wide range of hazards from both physical attacks as well as cyberthreats. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy or threaten the delivery of essential services such as drinking water and wastewater.

As with any critical enterprise or corporation, drinking water and wastewater utilities must evaluate and mitigate their vulnerability to a cyber incident and minimize impacts in the event of a successful attack. Impacts to a utility may include, but are not limited to:

- Interruption of treatment, distribution or conveyance processes from opening and closing valves, overriding alarms or disabling pumps or other equipment
- Theft of customers' personal data such as credit card information and social security numbers stored in on-line billing systems
- Defacement of the utility's website or compromise of the email system
- Damage to system components
- Loss of use of industrial control systems (e.g., SCADA system) for remote monitoring of automated treatment and distribution processes

Cyber incidents can compromise the ability of water and wastewater utilities to provide clean and safe water to customers, erode customer confidence and result in financial and legal liabilities. The following sections outline actions drinking water and wastewater utilities can take to prepare for, respond to and recover from cyber incidents.

Actions to Prepare for a Cyber Incident

Utility

- [ ] Identify all mission critical information technology (IT) systems, considering business enterprise, process control and communications. Document the key functions of the mission critical objectives, and identify the personnel or entity responsible for operating and maintaining each IT system.

- [ ] Identify an overall IT security lead to coordinate with each IT system manager and oversee all cyber-related duties.

- [ ] Ensure that IT system managers enforce cybersecurity practices on all business enterprise, process control and communications systems. For example, verify adherence to user authentication, current anti-virus software and installation of security patches.

- [ ] Identify priority points of contact for reporting a cyber incident and requesting assistance with response and recovery. Include any state resources that may be available such as State Police, National Guard Cyber Division or mutual aid programs, as well as the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) at https://www.cisa.gov/reporting-cyber-incidents.

- [ ] Review and update the utility's emergency response plan (ERP) to address a cyber incident impacting business enterprise, process control and communications systems. Account for all potential impacts on operations, and ensure emergency contacts are current.

- [ ] Prevent unauthorized physical access to IT systems through security measures such as locks, sensors and alarms. Include workstations and process control systems (e.g., programmable logic controllers or PLCs).

- [ ] Train all essential personnel to perform mission critical functions during a cyber incident that disables business enterprise, process control and communications systems. Include the manual operation of water collection, storage, treatment and conveyance systems.

- [ ] Conduct drills and exercises for responding to a cyber incident that disables critical business enterprise, process control and communications systems.

Actions to Prepare for a Cyber Incident *(continued)*

IT Staff or Vendor

- ☐ Establish a program for maintaining updated anti-virus software on all critical IT systems, along with rapid installation of all security patches.
- ☐ Set up an automatic back-up on critical systems and ensure the process is producing a readable, uncorrupted restore file on a routine basis.
- ☐ Implement rigorous user authentication, including multi-factor authentication where possible. Use individual accounts and unique passwords for each employee, and restrict IT system access privileges to the level needed for a user's duties.
- ☐ Restrict internet access to process control systems unless absolutely necessary.
- ☐ Where possible, separate process control system traffic from business traffic through the use of a firewall. If this is not possible, logically filter traffic through the use of a firewall.
- ☐ Identify all routes of remote access to IT systems. Eliminate remote access where possible, and restrict remaining access (e.g., do not allow persistent remote access to control networks).
- ☐ Assess the use of additional strategies to protect IT systems, such as application whitelisting, network segmentation with restricted communication paths and active monitoring for adversarial system penetration.
- ☐ Conduct a detailed assessment of vulnerabilities in all mission critical IT systems. Consider use of the tools and subject matter experts provided by the DHS Cybersecurity and Infrastructure Security Agency (https://www.cisa.gov/cybersecurity). Develop an action plan to mitigate all significant vulnerabilities identified in the assessment.

Notes:

Actions to Respond to a Cyber Incident

Utility

- [ ] If possible, disconnect compromised computers from the network to isolate breached components and prevent further damage, such as the spreading of malware. Do not turn off or reboot systems – this preserves evidence and allows for an assessment to be performed.
- [ ] Notify IT personnel and/or IT vendor of the incident and the need for emergency response assistance. In addition, DHS CISA can assist with IT system response and recovery (https://www.cisa.gov/reporting-cyber-incidents).
- [ ] Assess any damage to utility systems and equipment, along with disruptions to utility operations.
- [ ] Execute the utility ERP as needed, including notification of utility personnel, actions to restore operations of mission critical processes (e.g., switch to manual operation if necessary), and public notification (if required).
- [ ] Report the cyber incident as required to law enforcement and regulatory agencies.
- [ ] Notify any external entities (e.g., vendors, other government offices) that may have remote connections to the affected network(s).
- [ ] Document key information on the incident, including any suspicious calls, emails, or messages before or during the incident, damage to utility systems, and steps taken in response to the incident (including dates and times).

IT Staff or Vendor

- [ ] Review system and network logs, and use virus and malware scans to identify affected equipment, systems, accounts and networks.
- [ ] Document which user accounts were or are logged on, which programs and processes were or are running, any remote connections to the affected IT systems or network(s) and all open ports and their associated applications.
- [ ] If possible, take a "forensic image" of the affected IT systems to preserve evidence. Tools to take forensic images include Forensic Tool Kit (FTK) and EnCase.
- [ ] If possible, identify any malware used in the incident, any remote servers to which data may have been sent during the incident, and the origin of the incident. DHS CISA can assist with the forensic analysis (www.cisa.gov/reporting-cyber-incidents).
- [ ] Research and identify if any employee or customer personally identifiable information (PII) was compromised.
- [ ] Check the system back-up time stamp to determine if the back-up was compromised during the incident.
- [ ] Document all findings, and avoid modifying or deleting any data that might be attributable to the incident.

Notes:

Actions to Recover from a Cyber Incident

Utility

- [ ] Continue to work with IT staff, vendors and integrators, government partners and others to obtain needed resources and assistance for recovery.
- [ ] Notify affected employees and customers if any PII was compromised.
- [ ] Submit an incident report through WaterISAC (866-H2O-ISAC). Membership is not required to submit a report.
- [ ] Develop a lessons learned document and/or an after action report (AAR) to document utility response activities, successes, and areas for improvement. Create an improvement plan (IP) based on your AAR and use the IP to update your vulnerability assessment, ERP and contingency plans.
- [ ] Register for cybersecurity alerts and advisories from water sector and government partners to be aware of new vulnerabilities and threats. Two sources of cybersecurity alerts are WaterISAC, which has a basic membership that is free, and ICS-CERT (https://ics-cert.us-cert.gov/alerts).

IT Staff or Vendor

- [ ] Remove any malware, corrupted files and other changes made to IT systems by the incident.
- [ ] Restore IT systems as required (e.g., re-image hard drives, reload software). DHS CISA can assist with the IT system recovery (https://www.cisa.gov/reporting-cyber-incidents).
- [ ] Restore compromised files from a system back-up that has not been compromised.
- [ ] Install patches and updates, disable unused services and perform other countermeasures to harden the system against known vulnerabilities that may have been exploited.

Notes:

My Contacts and Resources

CONTACT NAME	UTILITY/ORGANIZATION NAME	PHONE NUMBER
	Law Enforcement	
	IT Staff/Vendor	
	SCADA Staff/Vendor	
	DHS Cybersecurity and Infrastructure Security Agency (CISA)	
	Local Laboratory	
	State Primacy Agency	
	Local Emergency Management Agency	
	Local Health Department	
	WARN Chair	
	State Emergency Management Agency	

Resources

- Best Cybersecurity Practices (Water ISAC)
- Cyber Security Evaluation Tool (DHS ICS-CERT)
- Advisories (DHS ICS-CERT)
- Cybersecurity Advisors (DHS)
- DHS Cybersecurity and Infrastructure Agency (CISA)
- Cybersecurity Guidance and Tool (AWWA)

Notes:

OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
24 FEBRUARY 2025 DHS-IA-IF-2025-05566

CYBERSECURITY

(U//FOUO) Cyber Attacks Against US Water and Wastewater Systems Sector To Continue Unless Vulnerabilities Mitigated

(U//FOUO) ***Scope Note:*** *This product responds to requests from state, local, and private industry stakeholders for a more in-depth look into the threat flagged in previous production regarding cyber attacks targeting the Water and Wastewater Systems Sector.[a] It also offers detailed mitigation options for stakeholder personnel responsible for technology maintenance and operation.*

(U//FOUO) **Malicious cyber actors will almost certainly continue exploiting any shortcomings in the cyber hygiene practices of US Water and Wastewater Systems (WWS) Sector entities to disrupt sector operations.** Malicious cyber actors find the sector an attractive target because they can take advantage of the sector's need for continuous operations, which hinders the ability of US WWS utilities to apply software patches and updates to their operational technology (OT).

- (U//FOUO) In recent years, malicious cyber actors on several occasions have leveraged gaps in the cyber hygiene practices of US WWS entities to cause kinetic impacts using unsophisticated cyber tactics. Between January and June 2024, for example, a pro-Russia criminal hacktivist group compromised the OT devices of four US WWS utilities using default credentials that were left unchanged. The criminal hacktivist group manipulated the devices to cause storage tank spills, according to DHS reporting.
- (U//FOUO) Malicious cyber actors do not need to explicitly manipulate operational processes or control OT devices to disrupt operations. In November 2023, Iranian government-affiliated cyber actors defaced OT devices that monitored, but did not control, processes at multiple US WWS entities, according to DHS reporting. In response, several victim utilities reverted to manual operations out of an abundance of caution, which requires more resources and personnel. Similarly, in September 2024, a ransomware attack against a US WWS utility

[a] (U//FOUO) For more information on threats to the US WWS Sector, please see I&A product, "Malicious Cyber Actors Likely View US Water and Wastewater Systems Sector as an Attractive Target," DHS-IA-IF-2023-18159, dated 24 October 2023.

prompted the utility to shift to precautionary manual operations, according to reporting from DHS, open-source reporting, and WaterISAC—a US WWS Sector security association comprised of member utilities from the United States and select partner nations.

- *(U//REL TO USA, FVEY)* People's Republic of China (PRC) state-sponsored cyber actors have compromised the information technology (IT) environments of multiple US WWS networks and have used their access to explore the networks, exfiltrate data, and harvest credentials, according to DHS reporting. The US government assesses that these actors are pre-positioning themselves on the IT networks of US critical infrastructure to enable lateral movement to OT and then disrupt key sector functions in the event of geopolitical tensions or conflict, according to a joint CISA advisory.
- *(U)* Cybersecurity in the US WWS Sector is expensive to maintain and difficult to apply because patches, updates, and other mitigation measures typically require system downtime that could impact utility operations, according to a US government report. The US WWS Sector is broad and consists of utilities with varying sizes, populations served, and cybersecurity budgets and capabilities. It is comprised of approximately 150,000 public water systems, which operate independently with their own processes, budgets, and technologies. Many US WWS utilities use OT for many processes, including source water intake; chemical distribution and other treatment steps; distribution; water storage; pumps; and monitoring, according to Environmental Protection Agency (EPA) guidance. Common OT systems in the US WWS Sector include industrial control systems (ICSs), human machine interfaces (HMIs), programmable logic controllers (PLCs), and remote terminal units, according to the same guidance.

(U) Appendix A: Potential Operational Technology Attack Vectors and Vulnerabilities

(U//FOUO) CISA has documented multiple common vulnerabilities and exploits in OT systems frequently employed by US WWS utilities. Utilities should particularly avoid using legacy ICS and HMI devices or those using default or weak passwords without multifactor authentication (MFA), according to CISA. Additionally, some foreign-manufactured devices—especially those made in the PRC—may be inherently vulnerable or are on the Federal Communication Commission list of banned devices that cannot be used in critical infrastructure, according to CISA. The below table itemizes Common Vulnerabilities and Exposures (CVEs) in WWS OT systems. The CVEs catalogue the details of publicly disclosed cybersecurity vulnerabilities and can be found on www.CVE.org or through the CISA Known Exploited Vulnerabilities (KEVs) Catalog at www.cisa.gov/known-exploited-vulnerabilities-catalog.

OVERALL TABLE CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

Vendor/Technology:	Vulnerabilities/Exploits:
Virtual Network Computing (VNC)	Check Specific VNC Vendor
Unitronics PLC	CVE-2023-6448
Robustel	Check Specific Versions
Sierra Wireless Hosts	Check Specific Versions
Hikvision Closed-Circuit Television (CCTV) Cameras	Check Specific Versions
Ivanti Connect Secure Virtual Private Network (VPN)	Check Specific Versions
Modbus	Verify Specific Vendors
Rockwell Automation ICSs	CVE-2021-22681 CVE-2022-1159 CVE-2023-3595 CVE-2023-3596 CVE-2023-46290 CVE-2024-21914 CVE-2024-21915 CVE-2024-21917

Apache	CVE-2021-40438 CVE-2021-44228 CVE-2017-12617 CVE-2020-1938
Cisco	CVE-2020-3452 CVE-2020-3580 CVE-2019-1653
Microsoft Exchange	CVE-2021-34473
NodeJS	CVE-2021-21315
PHP	CVE-2012-1823
SpringFramework	CVE-2022-22965

(U) Appendix B: CISA Recommendations for Mitigation

(U) The following mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA. The CPGs provide a minimum set of practices and protections that CISA recommends all organizations implement. CISA based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals (www.cisa.gov/cross-sector-cybersecurity-performance-goals) for more information on the CPGs, including additional, recommended baseline protections.

(U) **Identify:**

- *(U)* Take inventory and determine the end-of-life statuses for all HMIs. Replace end-of-life HMIs as soon as feasible. (CISA CPG 1.A)
- *(U)* Develop and maintain comprehensive documentation of assets and track current version and end-of-support (EOS) information for all software and firmware within the WWS. Regularly patch and update operating systems and applications as soon as updates become available to address known security vulnerabilities. (CISA CPG 1.A)
- *(U)* Develop and maintain comprehensive documentation of assets—tracking current version and EOS information for all operating systems and software within the WWS. Regularly patch and update operating systems and applications as soon as patches and updates become available to address known security vulnerabilities. (CISA CPG 1.A)
- *(U)* Develop and maintain comprehensive documentation of assets—tracking current version and EOS information for all software and firmware within the WWS. Regularly patch and update operating systems and applications as soon as patches or updates become available to address known security vulnerabilities. (CISA CPG 1.A)
- *(U)* Remediate all KEVs immediately, prioritizing critical assets. If a patch is available, entities should refer to vendor mitigation guidance and implement compensating controls to reduce risk of compromise. (CISA CPG 1.E)
- *(U)* Require active scanning for vulnerabilities and compliance in web applications, pushing developers to prioritize security. Mandate penetration testing by covering white box, black box, and cloud assets before implementation and as an ongoing practice. Establish clear expectations for web application service providers/vendors to conduct regular security testing. (CISA CPGs 1.E, 1.F, and 1.I)

- *(U)* Prioritize the importance of purchasing Secure by Design products. Require that documents and contracts with vendors and/or service providers opt for more secure offerings and include notifications of security incidents and security vulnerabilities within a risk-informed time frame. (CISA CPGs 1.G, 1.H, and 1.I)

(U) **Protect:**

- *(U)* Secure user access and restrict the exposure of credentials. Install a centralized identity and access management system to monitor and manage roles and access privileges of individual network entities for on-premises and cloud software. (CISA CPG 2.A)
- *(U)* Immediately change all default passwords on HMIs and use a strong, unique password. Ensure the factory default password is not in use. Open the remote settings panel to confirm the old password is no longer shown. (CISA CPGs 2.A and 2.B)
- *(U)* Change default passwords for new and existing OT devices. Use unique, strong passwords and MFA where technically feasible. (CISA CPGs 2.A, 2.B, 2.C, and 2.H)
- *(U)* Strengthen account security to include phishing-resistant MFA, the separation of user and privileged accounts, strong passwords, unique credentials, and a policy to revoke credentials for departing employees. (CISA CPGs 2.A, 2.B, 2.C, 2.D, 2.E, 2.G, and 2.H)
- *(U)* Implement multi-layered network defenses that combine the use of next-generation firewalls (NGFWs) and web application firewalls (WAFs) to filter and monitor traffic between a web application and the internet. Ensure that all firewalls are properly configured (strong authentication and passwords) and place web servers in a dedicated demilitarized zone to isolate internet traffic and prevent unauthorized access to the organization's networks. (CISA CPGs 2.B and 2.F)
- *(U)* Strengthen web application security by implementing security.txt files and WAFs to facilitate transparent vulnerability disclosure practices and to filter and monitor traffic between web applications and the internet. (CISA CPGs 2.B and 2.F)
- *(U)* Maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., business e-mail and web browsing). Implement time-based access for privileged accounts and minimize unnecessary privileges for users. All privileges should be reevaluated on a recurring basis to validate continued need for a given set of permissions. (CISA CPG 2.E)

- *(U)* Strengthen account security by separating user and privileged accounts, implementing phishing-resistant MFA, and establish monitoring for unusual activity to effectively enhance access control. (CISA CPGs 2.E and 2.H)
- *(U)* Prohibit the exposure of OT devices and vulnerable services from the public internet. When exposure is necessary, use security monitoring tools (Security Information and Event Management [SIEM] and/or NGFWs) to detect suspicious activity and only use remote access tools securely configured with MFA and managed access privileges to reduce exposure and accessibility. (CISA CPG 2.F)
- *(U)* Implement network segmentation to isolate critical systems from the corporate network to reduce the likelihood of threat actors accessing the OT network if the IT network has been compromised. (CISA CPG 2.F)
- *(U)* Establish network segmentation to minimize network infrastructure vulnerability to reduce risk of potential compromise. (CISA CPG 2.F)
- *(U)* Consider the implementation of an Endpoint Detection and Response solution to monitor end-user devices for anomalies and threats targeting sensitive data. (CISA CPGs 2.G, 2.T, and 2.U)
- *(U)* Implement MFA for all access to the OT network. For additional information, see CISA's More than a Password. (CISA CPG 2.H)
- *(U)* Implement phishing-resistant MFA for access to assets using the strongest available method for that asset, including hardware-based, mobile app-based, and lastly MFA via short message service. (CISA CPG 2.H)
- *(U)* Implement strong and up-to-date encryption protocols, such as Transport Layer Security (TLS), to secure sensitive data and maintain the integrity of IT and OT traffic. (CISA CPG 2.K)
- *(U)* Update all outdated or weak encryption and maintain properly configured and up-to-date Secure Sockets Layer/TLS encryption to protect data at rest and in-transit. (CISA CPG 2.K)
- *(U)* Ensure proper storage and access management for all sensitive information, including credentials. Sensitive data, including credentials, should not be stored in plaintext, and should only be accessed by authenticated and authorized users. (CISA CPG 2.L)
- *(U)* Establish and maintain secure configuration baselines for applications and services. (CISA CPG 2.O)
- *(U)* Update network diagrams to reflect both the IT and OT networks. (CISA CPG 2.P)

- *(U)* Implement a policy that requires approval before installing any new or updated hardware, firmware, or software on your organization's network to increase visibility into deployed assets and reduce the likelihood of compromise through installation of unapproved assets. (CISA CPG 2.Q)
- *(U)* Create backups of the engineering logic, configurations, and firmware of HMIs to enable fast recovery. Familiarize your organization with factory resets and backup deployment. (CISA CPG 2.R)
- *(U)* Ensure business critical systems and resources are backed up and encrypted on a regular basis. Backups should be encrypted and stored separately from the source systems and tested on a recurring basis. (CISA CPG 2.R)
- *(U)* Practice, maintain, and regularly update cybersecurity incident response plans for relevant threat scenarios to respond effectively and efficiently to cyber attacks and maintain business operations. (CISA CPG 2.S)
- *(U)* Log remote logins to HMIs, taking note of any failed attempts and unusual times. (CISA CPG 2.T)
- *(U)* Collect and store access and security-focused logs in a central system, such as a SIEM tool. Only authorized and authenticated users should access or modify logs, which should be securely stored for a duration informed by risk or regulatory guidelines. (CISA CPGs 2.T and 2.U)
- *(U)* Ensure unauthorized portable media devices and hardware are not connected to IT assets to prevent threat actors from gaining initial access or exfiltrating data through unauthorized devices. (CISA CPG 2.V)
- *(U)* Strengthen security and reduce the potential risk of threat actors gaining initial access through exploitation of vulnerable services such as Remote Desktop Protocol, File Transfer Protocol, and Telnet by implementing compensating controls for vulnerable services. Controls include implementing IP security through VPN or secure shell (SSH) protocols, enabling network-level authentication for user verification, enforcing the principle of least privilege to limit user access, performing session monitoring via privileged access management solutions to establish session management limitations, and changing default port settings to dynamic ports for additional server protection. (CISA CPG 2.W)
- *(U)* Disconnect all HMIs, such as the touchscreens used to monitor or make changes to the system, or PLCs, from the public-facing internet. If remote access is necessary, implement a firewall and/or VPN with MFA to control device access. (CISA CPGs 2.W and 2.X)

- *(U)* Prohibit exposure of OT devices and vulnerable services to the public internet. When exposure is necessary, use security monitoring tools (SIEM and/or NGFWs) to detect suspicious activities and use remote access tools securely configured with MFA and managed access privileges to reduce exposure and accessibility. (CISA CPG 2.X)
- *(U)* Continuously scan for assets and limit OT connections to the public internet, ensuring that OT assets remain offline unless necessary, with clear justifications and documentation. Implement continuous vulnerability detection measures to identify security risks. (CISA CPG 2.X)

(U) **Detect:**

- *(U)* Maintain a documented list of relevant threats and cyber actor tactics, techniques, and procedures and ensure proper detection methods. (CISA CPG 3.A)

(U) **Respond:**

- *(U)* Strengthen web application security by implementing security.txt files and WAFs to filter and monitor traffic between web applications and the internet. (CISA CPG 4.C)

(U) **Recover:**

- *(U)* Practice and maintain the ability to operate systems manually. (CISA CPG 5.A)
- *(U)* Additional Recommendations:
    - *(U)* Establish an allow list that permits only authorized device IP addresses.
    - *(U)* Check the integrity of PLC ladder logic or other PLC programming languages and diagrams to ensure they operate, especially if an intrusion has been identified.
    - *(U)* Keep VNC updated with the latest version available and ensure all systems and software are up to date with patches and necessary security updates.
    - *(U)* Implement software and hardware limits to the manipulation of physical processes where possible, limiting the impact of a successful compromise.

(U) **Device Manufacturers:**

(U) While critical infrastructure organizations can take steps to mitigate risks, it is ultimately the responsibility of the device manufacturer to build products that are

Secure by Design and default. The authoring organizations urge device manufacturers to take ownership of the security outcomes of their customers in line with the joint guide, Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software and CISA's Secure by Design webpage (www.cisa.gov/securebydesign).

- *(U)* **Eliminate default passwords.** The use of default credentials is a top weakness that threat actors exploit to gain access to systems. Manufacturers can eliminate this problem at scale through any of the approaches recommended in CISA's Secure by Design Alert.
- *(U)* **Mandate MFA for privileged users.** Changes to engineering logic or configurations are safety-impacting events in critical infrastructure. Any changes should require MFA.
- *(U)* **Include logging at no additional charge.** Change and access control logs allow operators to track safety-impacting events in their critical infrastructure. These logs should be free and use open standard logging formats.
- *(U)* **Publish software bills of materials (SBOM).** Vulnerabilities in underlying software libraries can affect wide swathes of devices. Without an SBOM, it is near impossible for a critical infrastructure system owner to measure and mitigate the impact a vulnerability has on their existing systems.

(U) Additionally, see CISA's Secure by Design Alert (www.cisa.gov/securebydesign/alerts) for details on how software manufacturers can shield web management interfaces from malicious cyber activity. By using Secure by Design tactics, software manufacturers can make their product lines secure "out of the box" without requiring customers to spend additional resources making configuration changes, purchasing tiered security software and logs, monitoring, and making routine updates.

(U) Additional Resources

(U//FOUO) For additional resources, please refer to the following:

- *(U)* CISA; "Cybersecurity Advisors" at https://www.cisa.gov/about/regions
- *(U)* EPA; "Cybersecurity Technical Assistance Program for the Water Sector" at https://www.epa.gov/waterresilience/forms/cybersecurity-technical-assistance-program-water-sector
- *(U)* CISA, EPA; "Water and Wastewater Systems Sector Toolkit" at https://www.cisa.gov/water
- *(U)* CISA, EPA, FBI; "Top Cyber Actions for Securing Water Systems" at https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems
- *(U)* EPA; "Cybersecurity for the Water Sector" at https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
- *(U)* CISA; "Cross-Sector Cybersecurity Performance Goals" at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals
- *(U)* CISA; "More than a Password" at https://www.cisa.gov/MFA
- *(U)* CISA; "Cyber Hygiene Services" at https://www.cisa.gov/topics/cyber-threats-and-advisories/cyber-hygiene-services
- *(U)* CISA; "Shifting the Balance of Cybersecurity Risk - Principles and Approaches for Secure by Design Software" at https://www.cisa.gov/resources-tools/resources/secure-by-design
- *(U)* CISA; "Secure by Design and Default Webpage" at https://www.cisa.gov/securebydesign
- *(U)* CISA; "Secure by Design Alert - How Manufacturers Can Protect Customers by Eliminating Default Passwords" at https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-manufacturers-can-protect-customers-eliminating-default-passwords
- *(U)* CISA; "Secure by Design Alert - How Software Manufacturers Can Shield Web Management Interfaces from Malicious Cyber Activity" at https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-software-manufacturers-can-shield-web-management-interfaces-malicious-cyber

Reference and Dissemination Information

Feedback	*(U//FOUO)* Customers may submit feedback on DHS I&A Analytic products via the DHS I&A Evaluation Form located at the following addresses: • Unclassified: https://forms.office.com/g/FKkyksC3eg • SIPR / HSDN: https://go.sgov.gov/IAFeedback • JWICS / CLAN: https://go.intelink.ic.gov/IAFeedback
Definitions	*(U)* **Criminal Hacktivist:** An individual or group who gains unauthorized access to computer files or networks in order to further social or political goals, wholly or in part, through unlawful acts or criminal cyber activity. *(U)* **Human Machine Interface:** Software and hardware that allow human operators to monitor the state of a process, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. *(U)* **Industrial Control System:** An information system used to control industrial processes, such as manufacturing, product handling, production, and distribution. *(U)* **Programmable Logic Controller:** An industrial computer with various inputs and outputs, used to control and monitor industrial equipment based on custom programming. *(U)* **Remote Terminal Unit:** A microprocessor-based electronic device used in an ICS to connect hardware to a distributed control system or supervisory and control data acquisition system for monitoring purposes.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. *(U)* **To report a computer security incident, please contact CISA at 888-282-0870; or go to IRF Index - IRF. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* **To report this incident to the Intelligence Community, please contact your DHS I&A Field Intelligence Officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Intelligence Officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Warning Notices & Handling Caveats	*(U)* **Warning:** This information is provided only for intelligence purposes. It cannot be used in connection with any foreign or domestic court proceedings or for any other

legal, judicial, or administrative purposes.

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U//FOUO) This report includes sensitive technical information related to computer network operations that could be used against US Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, e-mail addresses, or user names identified in this document is strictly prohibited.

(U) All US person information has been minimized. Should you require US person information, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.