Technical Cybersecurity Support Plan for Public Water Systems - Report to Congress

Office of Water

EPA 817-R-22-002

August 2022

Contents

INTRODUCTION

The *Infrastructure Investment and Jobs Act* (Public Law No. 117-58) (hereinafter, Bipartisan Infrastructure Law or BIL) requires the U.S. Environmental Protection Agency (EPA), in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), to develop a Technical Cybersecurity Support Plan (hereinafter, Support Plan). The BIL directs that "the Administrator [EPA], in coordination with the Director [CISA] and using existing authorities of [EPA] and [CISA] for providing voluntary support to public water systems and the Prioritization Framework, shall develop a Technical Cybersecurity Support Plan for public water systems." The Prioritization Framework is a separate document required under the BIL that describes a methodology for prioritizing public water systems (PWSs) for technical cybersecurity support. The Prioritization Framework is further described in Section 1 of this document.

Pursuant to the BIL, the Support Plan must address the following: "(i)…the methodology [as established by the Prioritization Framework] for identifying specific PWSs for which cybersecurity support should be prioritized, (ii)…timelines for making voluntary technical support for cybersecurity available to specific PWSs, (iii)…PWSs identified by [EPA], in coordination with [CISA], as needing technical support for cybersecurity, and (iv)…specific capabilities of [EPA] and [CISA] that may be utilized to provide support to PWSs…including (I) site vulnerability and risk assessments, (II) penetrations tests; and (III) any additional support determined to be appropriate by [EPA]." All support to PWSs under the Support Plan is voluntary.

As the Sector Risk Management Agency (SRMA) for the Water and Wastewater Systems sector, EPA leads the Federal effort to promote security and resilience, both physical and cyber, in water and wastewater systems and serves as a day-to-day Federal interface for coordination of sector-specific activities. In implementing its SRMA responsibilities, EPA collaborates with CISA and other Federal departments and agencies, along with state, local, Tribal, and territorial (SLTT) governments, private sector entities and associations, and critical infrastructure owners and operators. EPA provides, supports, and facilitates technical assistance to water and wastewater systems to identify and mitigate vulnerabilities and carries out incident management responsibilities consistent with statutory authority, including understanding the business or operational impact of a cyber incident on private sector critical infrastructure.

The authorities and responsibilities of EPA's SRMA mission stem from several statutes and Presidential Directives, including the *Homeland Security Act of 2002*, *America's Water Infrastructure Act of 2018*, the *National Defense Authorization Act (NDAA) of 2021*, Presidential Policy Directive 21 – *Critical Infrastructure Security and Resilience*, and Presidential Policy Directive 41 – *United States Cyber Incident Coordination*.

CISA under its authorities has responsibilities to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure in coordination with SRMAs. These responsibilities include identifying and prioritizing physical and cyber threats, vulnerabilities, and consequences to critical infrastructure; providing technical assistance to critical infrastructure owners and operators upon request; facilitating the exchange of intelligence to strengthen the security and resilience of critical infrastructure; and, pursuant to Presidential Policy Directive (PPD) 41, leading the Federal Government in critical infrastructure asset response through "furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents."

Not later than August 22, 2022, EPA must submit to the appropriate Congressional committees the Support Plan and a list describing any PWSs identified by EPA, in coordination with CISA, as needing technical support for cybersecurity. This list is attached as an appendix to the Support Plan.

SECTION 1: METHODOLOGY, AS ESTABLISHED BY THE PRIORITIZATION FRAMEWORK, FOR IDENTIFYING SPECIFIC PWSs FOR WHICH CYBERSECURITY SUPPORT SHOULD BE PRIORITIZED

Note: This section describes the Prioritization Framework, which EPA, in coordination with CISA, would use to prioritize PWSs where the need for technical assistance exceeds the near-term capacity to provide support. Section 3 of this Support Plan describes PWSs identified by EPA, in coordination with CISA, as potentially needing technical cybersecurity support at present. EPA published the Prioritization Framework as the *Prioritization Framework for Technical Cybersecurity Support to Public Water Systems*, EPA 817-R-22-001.

The Prioritization Framework is structured as a series of qualitative questions stemming from the criteria that the BIL requires EPA to consider. This qualitative structure will provide the flexibility necessary to tailor the prioritization of PWSs for technical cybersecurity support to specific threat circumstances and PWS' needs.

The Framework is not designed to assign a water system to a fixed prioritization rank independent of a scenario where prioritization is needed. Rather, it reflects the understanding that prioritizing PWSs for technical cybersecurity support will depend on the circumstances of a particular scenario (e.g., the type of cybersecurity vulnerability and technical support required, the number of water systems requesting assistance, and the capacity to deliver support).

Existing circumstances have not required the use of a prioritization framework. Should that need arise in the future, the Framework offered here could be adjusted as needed.

Under the Prioritization Framework, if demand for cybersecurity support exceeds near term capacity to respond, a PWS would be asked to respond to the prioritization questions. EPA, in coordination with CISA, would use those answers, as well as a number of other factors, to prioritize the requests for assistance. Some of those other factors may include:

- The risk to PWS operations and potential adverse impacts on the service area, downstream critical infrastructure, and defense/national security assets,
- The capabilities of a PWS to remediate the vulnerability without Federal support, and
- The risk reduction benefits that technical cybersecurity support would achieve.

Table 1 below lists the required statutory criteria for the Prioritization Framework, the associated questions that a PWS would answer when requesting cybersecurity technical support, and considerations for prioritizing the order of support.

Note that the order in which the criteria are listed in Table 1 does not imply preferential weighting for prioritization rank. Rather, weighting would be based on the threat circumstances and the needs of PWSs for technical cybersecurity support.

Table 1: PRIORITIZATION FRAMEWORK CRITERIA, QUESTIONS, AND AGENCY CONSIDERATIONS[1]

Statutory criteria from Sec. 1420A(b)(1)	**Questions for PWSs requesting technical cybersecurity support**	**Considerations for prioritizing assistance requests**
(A)…identify public water systems (including sources of water for those public water systems) that, if degraded or rendered inoperable due to an incident, would lead to significant impacts on the health and safety of the public	How many people does the PWS or source serve (including consecutive systems and those technologically integrated)? Does the service area have resources (e.g., alternative sources of supply) that could mitigate the impact of degraded water service? Note: Downstream critical infrastructure, such as health care, is addressed in a separate criterion.	Priority would increase with greater population served (i.e., adverse impacts from water service degradation would grow with higher population served). Priority would decrease for PWSs where the service area has greater resources to mitigate impacts of degraded water service.
(B)(i) whether cybersecurity vulnerabilities for a public water system have been identified under Section 1433	Did the PWS conduct a risk and resilience assessment under *America's Water Infrastructure Act* that included cybersecurity (required for community water systems serving over 3,300 people)? Did the PWS conduct an alternative cybersecurity vulnerability assessment (e.g., CISA Cyber Hygiene services, EPA Technical Assistance Provider program, NIST Cybersecurity Framework, or private sector assessment)?	Whether a PWS had conducted a cybersecurity vulnerability assessment would not be a factor in providing critical technical cybersecurity support. If a PWS reported that it had identified a vulnerability under an assessment but had not yet addressed the vulnerability, consider whether that vulnerability would increase the need for assistance under the threat circumstance. Regardless, the PWS would be encouraged to correct the deficiency. Furthermore, if a PWS requested technical cybersecurity support and had not assessed cybersecurity vulnerabilities, EPA, in coordination with CISA, would encourage the PWS to do so and would assist the PWS if necessary.

[1] **The Prioritization Framework criteria in this Table include minor modifications to the version submitted to Congress for the sake of clarity.**

Statutory criteria from Sec. 1420A(b)(1)	Questions for PWSs requesting technical cybersecurity support	Considerations for prioritizing assistance requests
(B)(ii) the capacity of a public water system to remediate a cybersecurity vulnerability without additional Federal support	What near- and long-term internal technical capabilities and financial resources does the PWS have to correct cybersecurity vulnerabilities? How urgent is the PWS's need for technical cybersecurity assistance? Are other external sources of technical cybersecurity support (e.g., other government or private sector assistance providers) available to the PWS?	A PWS with an urgent need for technical cybersecurity support (e.g., a known vulnerability that poses a significant risk to the PWS's operations) and that lacks either internal or external technical or financial resources to correct the vulnerability in a sufficient time frame would be prioritized for assistance.
(B)(iii) whether a public water system serves a defense installation or critical national security asset	Does the PWS serve a defense installation or national security asset (e.g., defense production facility, communications provider, etc.)?	Serving a defense installation or national security asset would be a significant prioritization factor for technical cybersecurity support.
(B)(iv) whether a public water system, if degraded or rendered inoperable due to an incident, would cause a cascading failure of other critical infrastructure	What critical infrastructure facilities does the PWS serve (across all 16 critical infrastructure sectors)?	PWSs that serve a greater number of critical infrastructure facilities would be prioritized for technical cybersecurity support. Further, PWSs that serve critical infrastructure facilities where a degradation in water service would cause especially severe consequences (e.g., health care facilities) would be prioritized for support.

SECTION 2: TIMELINES FOR MAKING VOLUNTARY TECHNICAL SUPPORT FOR CYBERSECURITY AVAILABLE TO SPECIFIC PWSs

Section 4 of this Support Plan, which describes specific capabilities of EPA and CISA that may be utilized to provide support to PWSs, includes both currently available support and planned future support. Separate timelines are associated with each.

The first part of Section 4 describes currently available support, which is listed on EPA's and CISA's websites and is available to any PWS upon request. As noted in Section 4, some of the currently available services are *self-assessments*, which would be conducted by the PWS and can be accessed at any time. Other services are *facilitated assessments*, which require coordination and must be scheduled.

Typically, the wait time to schedule facilitated assessments is minimal. For example, PWSs that register for EPA's Water Sector Cybersecurity Technical Assistance Provider Program are contacted within a few days for a preliminary assessment and to schedule a full assessment with a technical assistance provider. The vulnerability scanning and web application scanning offered by CISA typically begin within one week of a facility returning the appropriate forms.

The second part of Section 4 describes planned future support, which is targeted to the PWSs identified in Section 3 as having an elevated need for technical cybersecurity support. As described in Section 4, this support will comprise two areas:

1. "Checklist" of cybersecurity best practices coupled with training, which will be targeted to small community water systems[2] (serving 3,300 people or fewer) and all non-community water systems[3] that did not develop risk assessments and emergency response plans under America's Water Infrastructure Act of 2018, and
2. Technical support for PWSs to address vulnerabilities in current cybersecurity practices, which may be identified through a cybersecurity assessment program.

EPA intends to offer this support beginning in calendar year 2023. In 2022, EPA expects to develop the cybersecurity checklist guidance and training and build the capability to provide technical support for addressing cybersecurity deficiencies through a collaborative stakeholder process. These products and services would then be delivered when available in 2023 on an ongoing basis.

[2] Community water systems are PWSs (which are systems that have at least 15 service connections or regularly serve at least 25 individuals) that provide water to the same population year-round.

[3] Non-community water systems are composed of non-transient non-community water systems, which are PWSs that regularly supply water to at least 25 of the same people at least six months per year, but not year-round; and transient non-community water systems, which are PWSs that provide water in a place such as a gas station or campground where people do not remain for long periods of time.

SECTION 3: "PUBLIC WATER SYSTEMS IDENTIFIED BY EPA, IN COORDINATION WITH CISA, AS NEEDING TECHNICAL SUPPORT FOR CYBERSECURITY"[4]

Available data, discussed below, indicate that most PWSs need technical support for cybersecurity. However, certain PWSs may have an elevated need and would benefit from being targeted with specific additional resources.

In 2021, for example, a coalition of water sector associations collaborated on a survey of current cybersecurity practices, challenges, and needs of PWSs. The survey collected 606 responses from water and wastewater systems. The results showed that most PWSs had not implemented certain basic cybersecurity practices, such as identifying all network assets, and that many PWSs had not begun to conduct cyber protection efforts. Deficiencies in cybersecurity increased with decreasing water system size in terms of population served. Approximately half of respondents stated a need for technical assistance, advice, assessments, or other support along with training and education targeting the water sector (*Water and Wastewater Systems Cybersecurity 2021: State of the Sector*, Water Sector Coordinating Council, 2021).

The survey results are supported by evidence of the vulnerabilities that have been exploited in cyber-attacks on PWSs. In many incidents, threat actors used a lack of basic cybersecurity, such as the failure to update passwords or insecure remote access, to penetrate PWS networks. Cyber-attacks on PWSs are a national security concern due to the criticality of the water sector as lifeline infrastructure. Consequently, these incidents support the broad need for technical cybersecurity support across the water sector.

EPA has identified two situations where PWSs may have an elevated need for technical cybersecurity support:

1. Under America's Water Infrastructure Act of 2018, all community water systems serving over 3,300 people were required to conduct risk and resilience assessments that included computer and other automated systems and to address cybersecurity in emergency response planning. Consequently, smaller community water systems and all non-community water systems may not have undertaken these important security steps. As discussed in Section 4, EPA plans to develop a "checklist" of cybersecurity best practices and associated training to assist these PWSs with identifying and addressing cybersecurity vulnerabilities.
2. Where PWSs undergo a cybersecurity assessment and the assessment identifies vulnerabilities that need to be addressed, the PWS may request technical cybersecurity support. EPA plans to stand up a technical support service to provide individual assistance to PWSs with adopting cybersecurity practices to remediate the vulnerabilities.

By continuing to offer broad technical support for cybersecurity to all PWSs, along with targeted support to PWSs in situations like the two listed above that may have an increased need, EPA, in coordination with CISA and water sector partners, can reduce the risk and increase the resilience of the water sector to a potentially disabling cyber-attack.

[4] ***Safe Drinking Water Act*** **(42 U.S.C. 300g et seq.) Part B, Section 1420A(b)(2)(B)(iii), as amended by the** ***Infrastructure Investment and Jobs Act*** **(Public Law No. 117-58), Section 50113**

SECTION 4: "SPECIFIC CAPABILITIES OF EPA AND CISA THAT MAY BE UTILIZED TO PROVIDE SUPPORT TO PUBLIC WATER SYSTEMS"[5]

This section describes both the current resources available from EPA and CISA and the planned future work of EPA to provide technical cybersecurity support to PWSs. In addition to the resources described here, EPA emphasizes that many excellent cybersecurity standards, guidance materials, and risk management tools are available from other government agencies and private sector organizations, including the American Water Works Association, WaterISAC, and other water sector associations. Private sector products, however, are outside the scope of this document.

CURRENT RESOURCES

The Support Plan divides the technical cybersecurity support into four categories: *Assessments and Vulnerabilities, Industrial Control Systems (ICS)*, *Vendors/Third-Party Management*, and *Training Courses and Exercises*. These topic areas allow PWSs to quickly identify resources that address different types of threats and vulnerabilities that may be of concern.

Within the categories are subcategories, which may include *Prevention*, *Response*, or *Guidance*. *Prevention* describes resources intended to identify, prevent, and mitigate a cyber threat. These resources establish cyber hygiene, precede a cyber-attack, and aid in establishing resilient systems. The resources in this subcategory include assessments and vulnerabilities, checklists, alert systems, and playbooks available to PWSs.

The subcategory *Response* includes resources intended to help detect and contain malicious threats and restore normal operations following a cyber-attack. The resources help improve response time, limit the impact of cyber-attacks, and provide recovery resources. Provided resources include playbooks, software, cybersecurity exercises, and information sharing resources.

ASSESSMENTS AND VULNERABILITIES

The *Assessments and Vulnerabilities* section lists resources for voluntary assessments that are designed to prevent, deter, and mitigate risks of cyber-attacks on PWSs by identifying and addressing potential vulnerabilities that increase the likelihood of cyber-attacks. The resources in this section help PWSs make decisions about allocation of resources to enhance cybersecurity before an event and improve recovery following an event.

---

[5] ***Safe Drinking Water Act*** **(42 U.S.C. 300g et seq.) Part B, Section 1420A(b)(2)(B)(iv), as amended by the *Infrastructure Investment and Jobs Act* (Public Law No. 117-58), Section 50113**

For the listed resources, the Support Plan notes the level of expertise needed for each resource where applicable and whether the resource is a *self-assessment* or a *facilitated assessment*. *Self-assessments* can be conducted by the PWS itself, while *facilitated assessments* require additional coordination with EPA or CISA.

PREVENTION

Self-Assessments

Vulnerability Self-Assessment Tool (VSAT): This online self-assessment, provided by EPA, allows PWSs to identify the highest risks to mission-critical operations, including cyber risks, and find cost-effective measures to reduce the resulting risks. To start the assessment, review Conduct a Drinking Water or Wastewater Utility Risk Assessment and open the VSAT Web portal at https://vsat.epa.gov/vsat/.

Cybersecurity Evaluation Tool (CSET): A stand-alone desktop application that guides asset owners and operators through the process of evaluating operational technology (OT) and information technology (IT). Upon completion of the assessment, organizations will receive summarized and detailed findings. The CSET requires basic knowledge of the PWS networks and systems to complete. To get the desktop application, visit Downloading and Installing CSET | CISA.

Cyber Resilience Review (CRR): The CRR is an interview-based assessment that measures a PWS's operational and cybersecurity practices. The process measures the capabilities and capacities of the PWS to perform planning, manage, measure, and define cybersecurity across ten domains. This assessment is offered as a self-assessment and facilitated assessment. To utilize the self-assessment, review the below resources. To schedule a facilitated assessment, contact cyberadvisor@cisa.dhs.gov.

a. CRR – Question Set with Guidance
b. CRR – Self-Assessment
c. CRR – User Guide
d. CRR – NIST Cybersecurity Framework Crosswalks

Facilitated Assessments

Cybersecurity Assessment and Technical Assistance: A virtual or in-person EPA program offering free, confidential cybersecurity assessments to PWSs to lower impact and likelihood of a cyber incident. As a part of the program, the PWS will work to develop a cyber action plan with EPA and will work at its own pace to implement best practices. To learn more, review here.

Remote Penetration Testing (RPT): A CISA RPT team works with the PWS to test internet exposure to eliminate exploitable pathways. RPT focuses only on externally accessible systems. This is a remote process, not an on-site offering. This assessment requires a basic skill level to complete. View the Remote Penetration Fact Sheet for the detailed process or contact vulnerability@cisa.dhs.gov.

Vulnerability Scanning (VS): A CISA service continuously assessing the health of internet-accessible assets by initiating non-intrusive checks to determine potential vulnerabilities and configuration weaknesses. This assessment requires a basic skill level to complete. Review the Vulnerability Scanning Fact Sheet for the detailed VS process or email vulnerability@cisa.dhs.gov to request an assessment.

Phishing Campaign Assessment (PCA): A CISA service created to measure employees' tendency to click on email phishing lures. PCA tests the behavioral responses of a specified target user base. The findings are used to inform leadership of potential training and awareness improvements for the organization. The assessment only requires a basic skill level to complete. Review the Phishing Campaign Assessment Fact Sheet for detailed PCA process or contact vulnerability@cisa.dhs.gov to request an assessment.

Web Application Scanning (WAS): A CISA service that assesses the health of an organization's publicly accessible web applications and initiates non-intrusive checks to determine vulnerabilities, bugs, and weak configurations. WAS requires a basic skill level to complete. Review the detailed process in the Web Application Scanning Fact Sheet or contact vulnerability@cisa.dhs.gov.

Risk and Vulnerability Assessment: A CISA service comprised of virtual and on-site assessment that provides PWSs with an actionable risk analysis report containing remediation recommendations prioritized by risk and severity. Review the Risk and Vulnerability Assessment Fact Sheet for detailed information or contact vulnerability@cisa.dhs.gov.

Cyber Infrastructure Survey: A CISA survey evaluating the effectiveness of organizational security controls, cybersecurity preparedness, and the overall resilience of the organization's cybersecurity ecosystem. Upon completion of the survey, a user-friendly dashboard with results and findings will be provided. To schedule, contact cyberadvisor@cisa.dhs.gov.

Enhanced Cybersecurity Services (ECS): CISA services facilitating the protection of IT networks by offering intrusion detection and prevention services through approved service providers. The programs offer domain name service (DNS) sinkholing, email (SMTP) filtering, and NetFlow analysis. For specific program information contact ECS_Program@cisa.dhs.gov. For information on enrollment, contact an ECS service provider directly; service providers can be found at Enhanced Cybersecurity Services (ECS) | CISA.

Validated Architecture Design Review (VADR): A CISA assessment based on Federal and industry standards, guidelines, and best practices. The service includes architecture design review, system configuration and log review, and network traffic analysis to provide an in-depth analysis of infrastructure. Review FACT SHEET Validated Architecture Design Review for the detailed process. To schedule, contact vulnerability@cisa.dhs.gov.

RESPONSE

Facilitated Assessments

Red Team Assessment (RTA): A CISA service providing evaluation of an IT environment via simulations of advanced persistent threats (APTs). RTAs simulate APT tactics, techniques, and procedures to access, navigate, and persist in a stakeholder environment. RTA requires an advanced skill level to complete the assessment. Contact vulnerability@cisa.dhs.gov to request an RTA.

High Value Asset (HVA) Assessment: A CISA service assessing targeted critical assets through scenario-based penetration testing, web application testing, and social engineering to provide recommendations for system vulnerabilities. Review the detailed process in the HVA Fact Sheet or contact vulnerability_info@cisa.dhs.gov.

Malware Analysis: A CISA service that provides PWSs with a dynamic analysis of malicious code and recommendations for malware removal and recovery activity. To submit malicious code for analysis, visit https://www.malware.us-cert.gov.

GUIDANCE

Baseline Information on Malevolent Acts for Community Water Systems: This EPA document serves as a resource for PWSs to identify malevolent acts and take steps toward reducing the risks water systems will experience if a threat occurs or to potentially deter the threat. The document contains resources, questionnaires, and baseline information on cyber threats. To utilize the document, review Baseline Information on Malevolent Acts for Community Water Systems (epa.gov).

Guidance for Small Community Water Systems on Risk and Resilience Assessments under America's Water Infrastructure Act: This guidance document contains and explains the Risk and Resilience Assessments required for community water systems serving more than 3,300 but less than 50,000 people. It assists PWSs with assessing their risks from and resilience to malevolent acts, such as cyber-attacks, regardless of population size served. To access the assessment, review Guidance for Small Community Water Systems on Risk and Resilience Assessments under AWIA (epa.gov). Please note: this document is associated with the Baseline Information on Malevolent Acts for Community Water Systems provided above.

Water Sector Cybersecurity Brief for States: A brief from EPA and the Association of State Drinking Water Administrators providing information to help state primacy agencies start a conversation with PWSs about cybersecurity threats. Review the brief here: Water Sector Cybersecurity Brief for States (epa.gov).

Cybersecurity Incident Action Checklist: A customizable checklist from EPA to help PWSs prepare for, respond to, and recover from a cyber incident. To review the checklist, visit Water Sector Incident Action Checklist - Cybersecurity (epa.gov).

Free Cybersecurity Services and Tools: A list of no cost cybersecurity tools and resources to help organizations reduce the likelihood of a damaging cyber event, detect malicious activity, respond effectively to confirmed cyber incidents, and maximize resilience. To view the list of resources and tools, visit Free Cybersecurity Services and Tools | CISA.

INDUSTRIAL CONTROL SYSTEMS

Industrial Control Systems (ICS) are essential to the operation of U.S. critical infrastructure. ICS owners and operators face threats from a variety of adversaries whose intentions include theft, gathering intelligence, and disrupting National Critical Functions. As ICS owners and operators adopt new technologies to improve operational efficiencies, they should be aware of the additional cybersecurity risk of connecting OT to enterprise IT systems and Internet of Things (IoT) devices. This section will cover ICS prevention and response resources available to improve ICS protection.

PREVENTION

CISA Industrial Control Systems Security Offerings: CISA partners with the ICS community to help understand, detect, and protect against ICS risk and, when necessary, help critical infrastructure owners and operators respond to significant cybersecurity incidents. Review the cyber management products, services, and capabilities within the CISA Industrial Control Systems Security Offerings fact sheet. The included security offerings are as follows:

a. **Assessments:** Voluntary cybersecurity assessment services focused on OT that evaluate an organization's operational resilience, cybersecurity practices, management of external dependencies, and additional elements that are key to a robust cybersecurity framework. Visit https://www.cisa.gov/cyber-resource-hub for more information on how to request assessment services.

b. **Cyber Hunt:** CISA Cyber Hunt capabilities are specifically focused on identifying sophisticated threats and adversary presence in OT and IT environments, often beyond the capacity and capability of traditional cybersecurity tools and techniques.

c. **Exercises:** CISA provides cyber exercise planning to support ICS and critical infrastructure partners by delivering a full spectrum of cyber exercise planning workshops and seminars. These range from small discussion-based exercises that last two hours to full-scale, internationally scoped, operations-based exercises that span multiple days. The exercises were created to assist organizations at all levels in the development and testing of cybersecurity prevention, protection, mitigation, and response capabilities. For more information, visit https://www.cisa.gov/critical-infrastructure-exercises or email central@cisa.dhs.gov.

d. **Information Exchange:** CISA publishes ICS-specific alerts, advisories, and guidance documents for the public. The alerts provide timely notification to critical infrastructure owners and operators concerning control system threats. To view latest alerts, visit https://www.cisa.gov/ics.

e. **Partnerships and Engagement:** The Industrial Control Systems Joint Working Group (ICSJWG) supports information sharing and reduction of risk to the nation's ICS through enhanced collaboration between the Federal Government and private owners and operators of ICS across all critical infrastructure sectors. The working group offers in-person meetings, webinars, and newsletters. To learn about membership and events, visit https://www.cisa.gov/icsjwg.

f. **Response Capabilities:** CISA brings expertise and advanced tools to aid ICS cyber victims in identifying artifacts, determining affected components, and building recovery plans specific to lower-level OT devices. To report an ICS incident, visit https://www.cisa.gov/uscert/report.

g. **Strategic Risk Analysis:** CISA provides ICS partners with resources and capabilities to manage ICS risk through CISA's National Risk Management Center (NRMC). The NRMC serves as the end-to-end integrator of risk management activities for the National Critical Functions (NCFs) and leverages that risk expertise to support overall execution of the CISA mission. To access resources, visit https://www.cisa.gov/national-risk-management.

h. **Technical Analysis:** CISA's ICS advanced malware laboratory specializes in malware threats to ICS environments and can provide ICS owners and operators with support. To report malware, please visit https://www.cisa.gov/uscert/report.

i. **Training:** CISA's ICS training courses and workshops provide the ICS community no-cost, in-person, and virtual training. Learn more below or visit https://www.cisa.gov/cybersecurity-training-exercises to view training options.

j. **Vulnerability Coordination:** CISA's Coordinated Vulnerability Disclosure (CVD) program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). To report an ICS vulnerability, visit https://www.cisa.gov/uscert/report.

Known Vulnerabilities Catalog: A continually updated catalog that can be used by organizations to identify software updates per vendor instructions and fix known security flaws. To view the catalog, visit Known Exploited Vulnerabilities Catalog | CISA.

Malcolm: Malcolm is an open source, easily deployable network traffic analysis tool suite that enables the user to capture full network packet artifacts (PCAP files) and logs in OT/ICS environments. Malcom provides unique insight into specific protocols used in the ICS environments. Because Malcom comprises only open-source tools, it does not require users to obtain paid licenses. To learn more, contact central@cisa.dhs.gov.

Web-Based training on Industrial Control Systems: CISA training "Introduction to Control Systems Cybersecurity" will help ICS owners/operators to describe ICS deployments, components, and information flow; differentiate cybersecurity within IT and ICS domains; recognize sector dependencies; and identify cybersecurity resources within CISA. Courses are offered both online and in-person. Learn more information on the ICS training at Training Available Through CISA | CISA. Register for free ICS courses at CISA VLP (inl.gov).

RESPONSE

CyberSentry: A CISA-sponsored voluntary pilot program that leverages best in breed, commercial off-the-shelf technologies, such as network intrusion detection tools, to identify malicious activity in critical infrastructure ICS and corporate networks. CyberSentry participation increases real-time network visibility and the capability to detect nation-state adversaries, as well as derive cross-sector analytic insights. To learn more, contact central@cisa.dhs.gov.

GUIDANCE

Cybersecurity Best Practices for Industrial Control Systems: Guidance entailing the preventative steps ICS owners and operators can utilize to protect ICS in the event of a cyber-attack. The guidance breaks down cybersecurity best practices in various critical areas to increase ICS resilience. View the guidance here.

Securing Industrial Control Systems: The CISA guidance focuses on building ICS security capabilities that directly empower ICS stakeholders to secure their operations against threats. The intended audience is the whole ICS community and all CISA partners who have an interest in ICS security. This fact sheet is a summary of the strategy document. ICS Strategy Fact Sheet - Securing Industrial Control Systems: A Unified Initiative (cisa.gov).

Rising Ransomware Threat to OT Assets: CISA guidance providing resources for heightened awareness and voluntary recommendations for preparing for, mitigating, and responding to ransomware threats to OT. To learn more, visit CISA Fact Sheet: Rising Ransomware Threat to OT Assets.

Stopransomware.gov: StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively. Visit Stop Ransomware | CISA to learn more about how to prevent and recover from ransomware.

VENDOR/ THIRD-PARTY MANAGEMENT

Vendor and third-party organizations provide essential technology services to PWSs. However, as external dependencies, they also increase the risk of cyber threats and attacks. This section contains resources addressing the PWS' ability to prevent and respond to risks presented by external dependencies.

PREVENTION

CISA Coordinated Vulnerability Disclosure (CVD) Process: A CISA service that coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with affected vendor(s). The vulnerabilities cover ICS, IoT, and medical devices as well as traditional IT. To report an IoT or ICS vulnerability, email central@cisa.dhs.gov.

RESPONSE

External Dependencies Management (EDM) Assessment: An interview-based assessment that evaluates an organization's management of external dependencies. This assessment focuses on the relationship between an organization's high-value services and assets—such as people, technology, facilities, and information—and evaluates how the organization manages risks derived from its use of the Information and Communications Technology (ICT) Supply Chain in the deliverance of services. To schedule an assessment, contact cyberadvisor@cisa.dhs.gov.

a. EDM – Downloadable Resources: External Dependencies Management Assessment content and guides.

b. EDM – Assessment: Downloadable PDF Copy of the EDM Assessment so that a user can employ the EDM assessment for self-evaluation purposes for their organization. This assessment can be used as a precursor for on onsite assessment (facilitated by DHS Cybersecurity Advisor).

c. EDM – Assessment User's Guide: A guide containing the overall description of the EDM along with detailed steps and explanations for how to conduct an EDM self-assessment at an organization.

d. EDM – Question Set with Guidance: A guide containing the entire EDM assessment question set along with explanation on how to interpret and answer each of the questions contained within the self-assessment package.

TRAINING COURSES AND EXERCISES

Training courses and exercises provide PWSs with effective and practical mechanisms to identify best practices, lessons learned, and areas for improvement in plans and procedures. The exercises and training courses found within this section increase cybersecurity resilience within PWSs.

PREVENTION

Water Resilience Tabletop Exercise (TTX) Tool: An EPA tool providing PWSs with resources to plan, conduct, and evaluate tabletop exercises for all-hazards scenarios, including cybersecurity incidents.

CISA Tabletop Exercise (TTX) Packages (CTEPs): A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. Partners can use the exercises to initiate discussions within their organizations about their ability to address a variety of threat scenarios. The packages include pre-built templates for exercise planning, execution, and follow up. Below are the links to *Cybersecurity*, *Cyber-Physical*, and *Critical Infrastructure* scenarios. To review the pre-built documents, visit CISA Tabletop Exercises Packages | CISA.

a. **Cybersecurity Scenarios:** The Cybersecurity scenarios cover ICS, ransomware, ransomware of a third-party vendor, vendor phishing, water systems, and insider threats. Retrieve the Situation Manuals at Cybersecurity Scenarios | CISA.

b. **Cyber-Physical Convergence Scenarios:** The Cyber-Physical scenarios are designed to address the physical impacts resulting from a cyber threat or cyber impacts resulting from a physical threat. These scenarios are intended to further explore the impacts of convergence and how to enhance resiliency. To view the Situation Manuals, visit Cyber-Physical Convergence Scenarios | CISA.

c. **Critical Infrastructure Scenarios:** CISA assists government and industry partners in conducting exercises to enhance security and resilience of critical infrastructure. The exercises range from small-scale discussion-based exercises to large-scale operations-based exercises. For more information or to request services, please email cisa.exercises@cisa.dhs.gov.

Federal Virtual Training Environment (FedVTE): A free, online, and on-demand cybersecurity training system. With self-paced courses ranging from beginner to advanced levels, individuals can strengthen or build cybersecurity skillsets. To access the courses, visit FedVTE Login Page (usalearning.gov).

CISA Training: Web-based, self-paced, and instructor-led courses offered through CISA addressing cybersecurity and ICS support. Courses are located on the Virtual learning portal. Review the list of courses available at Training Available Through CISA | CISA.

Incident Response Training: CISA has developed no-cost cybersecurity incident response (IR) training for government employees and contractors across Federal and SLTT governments, and for educational and critical infrastructure partners. The course offerings range from basic to intermediate skill level. To review the list of webinars and events, visit Incident Response Training | CISA. To register for upcoming events, visit Connect Event Catalog (connectsolutions.com).

Cybersecurity Awareness Program: A national public awareness program to increase the understanding of cyber threats and empower the American public to be safer and more secure online. To learn more, visit CISA Cybersecurity Awareness Program | CISA.

Cyber Games: Each game presents simulated cybersecurity threats, defenses, and response actions. The games are available for download on Android and Apple iOS devices. To review and play the game options, visit Cyber Games | CISA.

Cyber Career Pathway Tools Fact Sheet: A CISA program that helps individuals identify, build, and navigate a potential cyber career pathway by increasing understanding of the knowledge, skills, and abilities needed to begin, transition, or advance a cyber career. To learn more, visit The Cyber Career Pathways Tool: The New Interactive Tool for Career Exploration (cisa.gov).

PLANNED FUTURE EPA TECHNICAL CYBERSECURITY SUPPORT FOR WATER SYSTEMS

As discussed in Section 3, EPA plans to develop additional technical cybersecurity support for PWSs in two situations:

Checklist of Cybersecurity Best Practices: This brief guidance document will be targeted to small community water systems (those serving 3,300 people or fewer) and all non-community water systems that may not have conducted a risk and resilience assessment and developed an emergency response plan for cyber threats under America's Water Infrastructure Act of 2018. It should be written for PWSs with low technical capability. EPA plans to accompany it with an online training course.

Cybersecurity Technical Support Service: EPA plans to offer a standing service where subject matter experts are available to offer technical advice to PWSs on approaches to mitigating vulnerabilities in current cybersecurity practices, which may be identified through the cybersecurity assessment program.

APPENDIX: PUBLIC WATER SYSTEMS IDENTIFIED BY EPA, IN COORDINATION WITH CISA, AS NEEDING TECHNICAL SUPPORT FOR CYBERSECURITY

As discussed in Section 3, available data indicate that most PWSs need technical support for cybersecurity. However, EPA has identified the following two categories of PWSs as potentially having an elevated need for additional technical support:

1. Community water systems serving 3,300 people or fewer and all non-community water systems were not required to conduct risk and resilience assessments or develop emergency response plans under America's Water Infrastructure Act of 2018. EPA believes that these steps are essential security measures. They are necessary for PWSs to identify and remediate their most significant vulnerabilities, both physical and cyber, and to be prepared to respond to a cyber-attack and minimize any disruption in service.

   To address this security gap, EPA plans to develop a "checklist" of cybersecurity best practices, along with guidance on how to implement them and associated training. While this checklist and guidance will be available to all PWSs, EPA plans to target the training to small community water systems and all non-community water systems, which will encourage these PWSs to identify and address cybersecurity vulnerabilities.

   Nationally, community water systems serving 3,300 people or fewer and all non-community water systems comprise approximately 145,000 PWSs in total. Consequently, EPA is not listing all these systems individually in this report. All PWSs in these categories may be identified through EPA's Safe Drinking Water Information System using this page: SDWIS Federal Reports Advanced Search (epa.gov).

2. A second category of PWSs that may need additional technical support for cybersecurity are those that undergo a cybersecurity risk assessment, which could be conducted by a Federal or SLTT entity under a regulatory program or voluntarily by the PWS or an outside technical assistance provider. A PWS may require technical support to address vulnerabilities that this assessment identifies. EPA plans to stand up a technical support service to provide individual assistance to PWSs (remotely) with adopting cybersecurity practices to remediate vulnerabilities. Because this support will be provided as requested by individual PWSs, EPA cannot identify in advance the specific PWSs that will need this support.