

CRITICAL INFRASTRUCTURE PROTECTION

EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems



Report to Congressional Requesters

August 2024
GAO-24-106744
United States Government Accountability Office

Accessible Version

GAO Highlights

View [GAO-24-106744](#). For more information, contact J. Alfredo Gómez at (202) 512-3841 or gomezj@gao.gov, or David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov
Highlights of [GAO-24-106744](#), a report to congressional requesters

August 2024

CRITICAL INFRASTRUCTURE PROTECTION

EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems

Why GAO Did This Study

Recent cyber incidents highlight the vulnerability of the 170,000 water and wastewater systems in the U.S. water sector. EPA is responsible for leading, coordinating, and supporting activities to reduce cybersecurity risk to the water sector. The agency works in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and other federal, state, and local entities.

GAO was asked to review cybersecurity threats facing the water sector and the federal government's efforts to address these threats. This report (1) describes cybersecurity risks and incidents; (2) examines actions by selected federal and nonfederal entities to improve cybersecurity; and (3) evaluates EPA's actions to address known risks.

GAO analyzed documents from EPA, CISA, and other entities on cyber threats, threat actors, and sector efforts to reduce risk. GAO interviewed federal and nonfederal officials with relevant cybersecurity responsibilities. GAO also visited and interviewed officials from large and small systems selected to provide varying perspectives.

What GAO Recommends

GAO is making four recommendations, including that EPA assess sector risk; develop and implement a national cybersecurity strategy; and evaluate the sufficiency of its legal authorities to carry out its cybersecurity responsibilities and seek additional authority as necessary. EPA concurred with the recommendations and said it is taking action to complete them.

What GAO Found

The water sector faces increasing cybersecurity-related risk. While national reporting requirements for cyber incidents are being developed, known incidents have disrupted water sector operations. Nations (including Iran and China), cybercriminals, and others have targeted water systems. For example, foreign hackers targeted multiple water systems in late 2023. Cyberattacks threaten public health, the environment, and other critical infrastructure sectors.

Water and Wastewater Systems' Vulnerability to Cyberattacks



Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/James Thew/stock.adobe.com (photos). | GAO-24-106744

Accessible Text for Water and Wastewater Systems' Vulnerability to Cyberattacks

- Water systems may contain hundreds of diverse components, making it difficult to properly map and keep operational technologies updated with security patches.
- Attackers may use IT networks to steal data or to move within the network to access operational systems.
- IT and operational networks may not be properly separated, allowing attackers to access the operational systems and disrupt critical processes.

Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/James Thew/stock.adobe.com (photos). | GAO-24-106744

Federal agencies and other entities have acted to improve water sector cybersecurity, but reported challenges such as workforce skills gaps and older technologies that are difficult to update with cybersecurity protections. Further, the sector has made limited investments in cybersecurity protections because water systems prioritize funding to meet regulatory requirements for clean and safe water, while improving cybersecurity is voluntary. In a May 2024 alert, the Environmental Protection Agency (EPA) said it planned to increase enforcement activities to ensure drinking water systems address cybersecurity threats.

EPA has assessed aspects of cybersecurity risk but has not conducted a comprehensive sector-wide risk assessment or developed and used a risk-informed strategy to guide its actions. EPA is required by law, as well as National Security Memorandum 22 (NSM-22), to identify, assess, and prioritize water sector risk. EPA official said they have assessed threats, vulnerabilities, and consequences, but have not integrated this work in a comprehensive assessment. Without a risk assessment and strategy to guide its efforts, EPA has limited assurance its efforts address the highest risks.

EPA has faced challenges using its existing legal authority and voluntary approaches to manage cybersecurity risks but has not fully evaluated either approach. In March 2023, EPA interpreted existing legal requirements to include cybersecurity assessments at drinking water systems but withdrew the requirement 7 months later after facing legal challenges. Previous requirements and NSM-22 direct EPA to identify the authorities it needs to compel the sector to address risks. In July 2024, EPA officials said they had evaluated their authorities and would release the evaluation in 2025 with their risk assessment and strategy. Doing so and seeking additional authority as necessary can help EPA ensure the water sector is better prepared for any future cyberattacks.

Contents

GAO Highlights	ii
Why GAO Did This Study	ii
What GAO Recommends	ii
What GAO Found	ii

Letter	1
Background	3
Water and Wastewater Systems Face Increasing Cybersecurity Risk and Cyber Incidents	10
Efforts to Improve Water Sector Cybersecurity Are Ongoing, but EPA Has Not Ensured a Key Risk Assessment Tool Produces Credible Results	20
EPA Has Not Developed a Cybersecurity Strategy or Fully Evaluated Its Legal Authorities to Address Water Sector Risks	28
Conclusions	35
Recommendations for Executive Action	35
Agency Comments	36

Appendix I	Objectives, Scope, and Methodology	38
Appendix II	Cyber Threat Techniques	42
Appendix III	Examples and Reported Numbers of Cybersecurity and Infrastructure Security Agency Security Assessments	43
Appendix IV	Actions Taken by State and Water Sector Organizations to Address Cybersecurity Risks	45
Appendix V	Comments from the Environmental Protection Agency	48
Accessible Text for Appendix V	Comments from the Environmental Protection Agency	
Appendix VI	GAO Contacts and Staff Acknowledgments	55

Tables	
Table 1: Examples of Actors That Can Threaten Water and Wastewater System Cybersecurity	11
Table 2: Potential Consequences of a Successful Cyberattack against Water and Wastewater Systems	19
Table 3: Potential Techniques Available to Cyber Attackers	42
Table 4: Examples of Cybersecurity and Infrastructure Security Agency (CISA) Security Assessments and Reported Numbers of Assessments Conducted for the Water Sector and All Other Sectors, Fiscal Years (FY) 2022 and 2023	43

Figures	
Water and Wastewater Systems' Vulnerability to Cyberattacks	iii

Accessible Text for Water and Wastewater Systems' Vulnerability to Cyberattacks	iii
Figure 1: Water and Wastewater Sector Infrastructure	4
Figure 2: Example of Water System Pipes, Pumps, and Tanks That Could Be Monitored or Controlled by Operational Technologies	5
Figure 3: Example of Monitoring Hardware and a Supervisory Control and Data Acquisition (SCADA) System Display in a Water Treatment Facility Control Room	6
Accessible Text for Figure 3: Example of Monitoring Hardware and a Supervisory Control and Data Acquisition (SCADA) System Display in a Water Treatment Facility Control Room	6
Figure 4: Examples of Water and Wastewater System Control Panels Containing Operational Technology Components	7
Accessible Text for Figure 4: Examples of Water and Wastewater System Control Panels Containing Operational Technology Components	7
Figure 5: Example of Water and Wastewater System Vulnerability to Cyberattack	14
Accessible Text for Figure 5: Example of Water and Wastewater System Vulnerability to Cyberattack	14

Abbreviations

AWIA	America's Water Infrastructure Act of 2018
CISA	Cybersecurity and Infrastructure Security Agency
CSA	cybersecurity advisor
DHS	U.S. Department of Homeland Security
EPA	U.S. Environmental Protection Agency
FBI	Federal Bureau of Investigation
Fiscal Year 2021 NDAA	William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021
NSM-22	National Security Memorandum on Critical Infrastructure Security and Resilience 22
NIST	National Institute of Standards and Technology
PFAS	per- and polyfluoroalkyl substances
PLC	programmable logic controller
PPD-21	Presidential Policy Directive-21
PSA	protective security advisor
SCADA	Supervisory Control and Data Acquisition
SDWA	Safe Drinking Water Act
USDA	U.S. Department of Agriculture
VSAT	Vulnerability Self-Assessment Tool
WaterISAC	Water Information Sharing and Analysis Center
WaterTA	Water System Technical Assistance

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



August 1, 2024

The Honorable Glenn Grothman
Chairman
The Honorable Robert Garcia
Ranking Member
Subcommittee on National Security, the Border, and Foreign Affairs
Committee on Oversight and Accountability
House of Representatives

The Honorable Stephen F. Lynch
House of Representatives

Cyberattacks are increasingly posing risks to the nation’s water and wastewater systems, which deliver clean and safe water essential for modern life and the U.S. economy. Safe drinking water is necessary for protecting public health, and properly treated wastewater is important for preventing disease and protecting the environment. However, cyberattacks on these systems can lead to service disruptions that harm public health or the environment. For example, a cyberattack could override the systems that monitor and control automated treatment processes, leading to unsafe levels of bacteria, parasites, or chemicals in drinking water. Cyberattacks resulting in unsafe water—or even the perception of unsafe water—can also erode public trust and faith in government.

Multiple federal, state, and local authorities responsible for public health, environmental protection, and security measures govern the nation’s water sector, which comprises approximately 170,000 systems—over 153,000 public drinking water systems and 16,500 public wastewater systems. As the Sector Risk Management Agency for the water sector, the U.S. Environmental Protection Agency (EPA) is responsible for coordinating water sector activities, conducting incident management activities, supporting sector risk management, and sharing information.¹ EPA is to carry out these responsibilities in collaboration with the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and other federal agencies, state and local governments, private sector entities and associations, and critical infrastructure owners and operators.

You asked us to review the cybersecurity threats that the water sector faces and the federal government’s efforts to address these threats. This report (1) describes cybersecurity risks and water sector incidents, (2) examines actions selected federal and nonfederal entities have taken to improve water sector cybersecurity,

¹6 U.S.C. § 650(23). The April 2024 White House National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) categorized the nation’s critical infrastructure into 16 sectors with at least one federal agency designated as Sector Risk Management Agency for the sector, although the number of sectors and Sector Risk Management Agency assignments are subject to review and modification. See 6 U.S.C. § 652a(b); The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (Washington, D.C.: Apr. 30, 2024) (rescinding and replacing the 2013 Presidential Policy Directive-21 (PPD-21)). The 16 critical infrastructure sectors are Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Health Care and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

and (3) evaluates the extent to which EPA has taken actions to address known cybersecurity risks to the water sector.

To address all three objectives, we analyzed documentation from relevant federal and state agencies, visited one drinking water and two wastewater systems that were selected to provide perspectives from large and small systems, interviewed federal and state officials, and interviewed nonfederal organizations and sector associations representing various aspects of the water sector.

To describe cybersecurity risks and water sector incidents, we reviewed publicly available threat reports as well as EPA, CISA, and other federal guidance and advisories. We also reviewed our prior reports on cybersecurity threats to critical infrastructure.² In addition, we interviewed federal and nonfederal officials to discuss cybersecurity threats, vulnerabilities, and the potential consequences of a successful cyberattack on the water sector.

To examine actions selected federal and nonfederal entities have taken to improve water sector cybersecurity, we reviewed documentation of efforts to share information, provide technical assistance, develop and share guidance, and deliver training. In addition, we interviewed federal and nonfederal officials to discuss steps that the water sector has taken to improve its cybersecurity. Specifically, we interviewed officials from federal entities with water sector cybersecurity responsibilities or programs. We also interviewed officials from a nongeneralizable sample of state water and wastewater regulatory agencies, sector associations, and water and wastewater system staff. We selected a nongeneralizable sample of states to include those states where known cyber incidents had affected drinking water or wastewater systems. We selected sector associations to obtain perspectives from different aspects of the water sector, such as wastewater, drinking water, large and small systems, and other variables.

To evaluate the extent to which EPA has taken actions to address known cybersecurity risks to the water sector, we reviewed documentation on actions that EPA has taken to identify and respond to cybersecurity risks. These documents included EPA memoranda, advisories, and planning documents. We also interviewed officials from EPA regarding agency actions to address cybersecurity risks. We compared EPA's actions with the Sector Risk Management Agency requirements in the Homeland Security Act of 2002, as amended by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), the critical infrastructure protection priorities in the 2023 National Cybersecurity Strategy, the sector risk assessment standards in the 2013 National Infrastructure Protection Plan, and GAO criteria for developing and implementing effective program strategies.³ We also reviewed the updated Sector Risk Management

²For example, see GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, [GAO-19-332](#) (Washington, D.C.: Aug. 26, 2019); *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, [GAO-21-81](#) (Washington, D.C.: Mar. 18, 2021); *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, [GAO-23-105789](#) (Washington, D.C.: Oct. 26, 2022); *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, [GAO-19-48](#) (Washington, D.C.: Dec. 18, 2018); and *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, [GAO-23-105468](#) (Washington, D.C.: Sept. 26, 2023).

³The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002(c)(1), 134 Stat. 3388, 4770-72 (2021) (amending the Homeland Security Act of 2002) (codified at 6 U.S.C. § 665d); The White House, *National Cybersecurity Strategy* (Washington, D.C.: March 2023); Department of Homeland Security, *NIPP [National Infrastructure Protection Plan] 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013); and GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004).

Agency requirements in the April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). Our complete scope and methodology is in appendix I.

We conducted this performance audit from April 2023 to July 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Water and Wastewater System Characteristics

The water sector is composed of drinking water and wastewater systems of varying sizes and ownership types. Multiple governing bodies (e.g., federal, tribal, state, local) are responsible for implementing public health, environmental protection, and security measures.

Drinking water. Approximately 153,000 public water systems provide drinking water to at least 15 service connections or regularly serve at least 25 people.⁴ A public water system may be publicly or privately owned. The majority of public water systems are considered small community water systems, serving fewer than 3,300 individuals. Specifically, about 80 percent of community water systems serve about 8 percent of the population.⁵ Conversely, less than 1 percent of community water systems serve populations over 100,000.

Wastewater. Over 16,500 publicly owned treatment facilities and a small number of private facilities treat the nation's wastewater.⁶ As with drinking water, there are relatively few very large wastewater systems as compared with the number of smaller systems. Specifically, about 79 percent of systems treat less than 1 million gallons of wastewater per day and collectively provide treatment to approximately 10 percent of the population. Utilities that treat more than 1 million gallons per day provide wastewater treatment to the other 90 percent of the population.

Water and Wastewater System Infrastructure and Technology

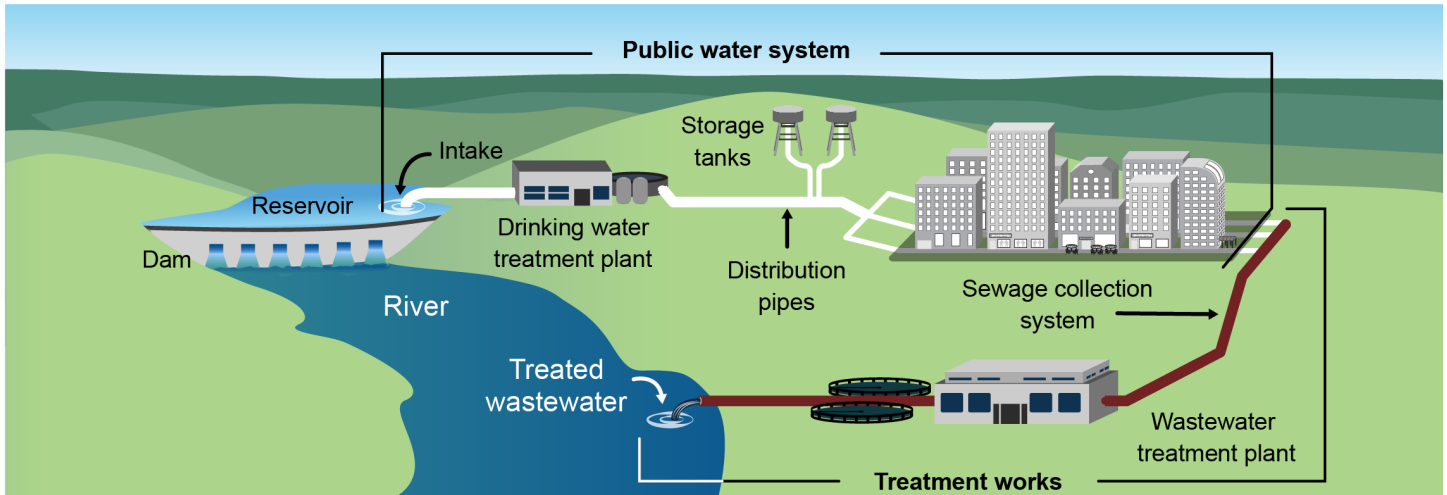
Water sector infrastructure is often widely dispersed, covering large geographic areas of piped distribution and collection networks connected to centralized treatment facilities, as depicted in figure 1.

⁴As defined by EPA, a public water system provides water for human consumption through pipes or other constructed conveyances to at least 15 service connections or serves an average of at least 25 individuals for at least 60 days per year. 40 C.F.R. § 141.2.

⁵EPA has defined three types of public water systems: (1) Community Water System—a public water system that serves at least 15 service connections used by year-round residents; (2) Non-Transient Non-Community Water System—a public water system that is not a community water system but still regularly serves at least 25 of the same people more than 6 months of the year (e.g., schools, office buildings); and (3) Transient Non-Community Water Systems—a public water system that is not a community water system that serves transient consumers, such as gas stations or campgrounds. See 40 C.F.R. § 141.2. See also Department of Homeland Security and Environmental Protection Agency, *Water and Wastewater Systems Sector-Specific Plan* (2015).

⁶Under the Clean Water Act regulations, EPA defines publicly owned treatment works as facilities that treat domestic sewage and that are owned by a municipality or state. See 40 C.F.R. § 501.2.

Figure 1: Water and Wastewater Sector Infrastructure



Sources: U.S. Environmental Protection Agency and Department of Homeland Security (information); GAO (graphic). | GAO-24-106744

Most water and wastewater systems rely on operational technology and IT systems to operate. Operational technology systems are programmed to provide remote and automated control of pipes, pumps, and other physical elements used to treat, store, distribute, and monitor water for contaminants or other properties, such as water pressure or quality. Department of Commerce’s National Institute of Standards and Technology (NIST) describes operational technology as a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment).⁷ These systems and devices detect or cause a direct change through monitoring or control of devices, processes, and events. Figure 2 shows an example of water system pipes, pumps, and tanks that could be monitored or controlled by operational technologies.

⁷National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*, Special Publication 800-82, Rev. 3 (Gaithersburg, Md.: September 2023).

Figure 2: Example of Water System Pipes, Pumps, and Tanks That Could Be Monitored or Controlled by Operational Technologies

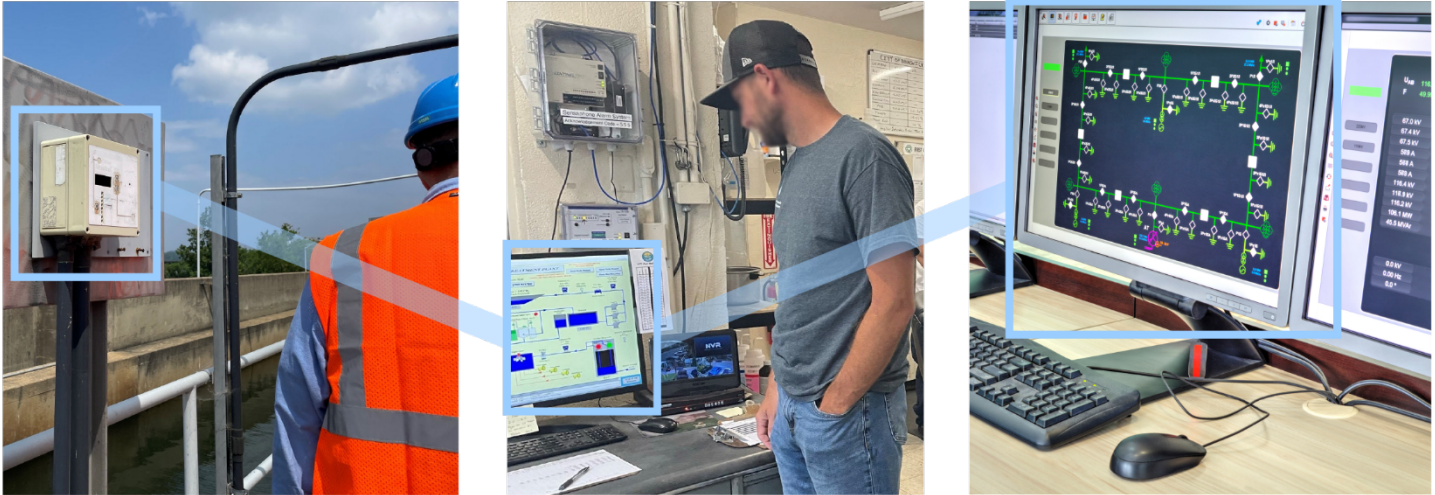


Source: qq47182080/stock.adobe.com. | GAO-24-106744

Many water and wastewater facilities use Supervisory Control and Data Acquisition (SCADA) systems, which are a component of operational technology that link monitoring and control systems. SCADA systems are made of hardware and software components that can collect, translate, and display real-time information for water system operators. For example, a SCADA system can monitor water levels in different tanks and can turn pumps on or off to move water through pipes, add chemicals, adjust water pressure, or conduct similar functions.

SCADA systems can automate certain functions or let operators know when changes are needed to certain processes. SCADA systems at some water and wastewater treatment facilities send information to a central display in a control or operations room, as shown in figure 3.

Figure 3: Example of Monitoring Hardware and a Supervisory Control and Data Acquisition (SCADA) System Display in a Water Treatment Facility Control Room



SCADA systems are made of hardware and software components working together to collect, translate, and display data. When abnormal conditions occur within a water treatment process, SCADA systems can trigger alarms to notify operators that something is wrong. SCADA may use wired or wireless technologies to transmit data between machines and operators.

Sources: Process Solutions, Inc. (information); GAO (left, middle photos), phadventure/stock.adobe.com (right photo). | GAO-24-106744

Accessible Text for Figure 3: Example of Monitoring Hardware and a Supervisory Control and Data Acquisition (SCADA) System Display in a Water Treatment Facility Control Room

SCADA systems are made of hardware and software components working together to collect, translate, and display data. When abnormal conditions occur within a water treatment process, SCADA systems can trigger alarms to notify operators that something is wrong. SCADA may use wired or wireless technologies to transmit data between machines and operators.

Sources: Process Solutions, Inc. (information); GAO (left, middle photos), phadventure/stock.adobe.com (right photo). | GAO-24-106744

SCADA hardware in a water system can include data collection devices, such as sensors, or data processing devices such as programmable logic controllers (PLC). PLCs collect data from inputs and sensors and translate that data into information that can be used by the SCADA system and understood by operators.⁸ SCADA systems can use wired or wireless technology to transmit data between machines and operators. Figure 4 shows examples of water system control cabinets that include operational technologies used to integrate information from sensors into information for operators.

⁸Process Solutions, Inc., *Functions and Components of a SCADA System* (Apr. 17, 2020).

Figure 4: Examples of Water and Wastewater System Control Panels Containing Operational Technology Components



Water and wastewater system operational technologies include devices to process data from sensors and other inputs, such as programmable logic controllers (PLC) (below). PLCs and other devices are stored in control cabinets (left) and can be programmed to monitor conditions and implement safety measures.

Sources: GAO analysis (information); GAO (left photo); xmentoys/stock.adobe.com (right photo). | GAO-24-106744

Accessible Text for Figure 4: Examples of Water and Wastewater System Control Panels Containing Operational Technology Components

Water and wastewater system operational technologies include devices to process data from sensors and other inputs, such as programmable logic controllers (PLC) (below). PLCs and other devices are stored in control cabinets (left) and can be programmed to monitor conditions and implement safety measures.

Sources: GAO analysis (information); GAO (left photo); xmentoys/stock.adobe.com (right photo). | GAO-24-106744

Water and wastewater facilities also use IT systems, which include customer billing, email, and other internet-based applications and tools. IT systems can be managed by the water or wastewater facility, by local municipalities (such as IT systems used to manage customer billing), or by private companies. IT systems can also include the electronic networks used to link monitoring and control systems for water treatment or distribution.

Selected Federal Laws Related to Drinking Water and Wastewater

Safe Drinking Water Act. The Safe Drinking Water Act (SDWA), as amended, requires EPA to establish legally enforceable standards for public water systems, which generally limit the levels of specific contaminants in drinking water that can adversely affect public health.⁹ EPA’s Office of Water has primary responsibility for

⁹Safe Drinking Water Act, Pub. L. No. 93-523, 88 Stat. 1660 (1974) (codified as amended 42 U.S.C. §§ 300f–300j-9). See 42 U.S.C. § 300g-1 (requiring EPA to issue national drinking water regulations).

implementing the requirements of the act. States authorized by EPA typically have the lead role in implementing and enforcing the resulting federal drinking water regulations, although EPA retains independent enforcement authority in certain areas.

America’s Water Infrastructure Act of 2018 (AWIA). AWIA amended section 1433 of SDWA to require each community water system serving more than 3,300 people to assess its risk to and resilience from “malevolent acts” (which include cyberattacks, as determined by EPA) and natural hazards and to prepare emergency response plans.¹⁰ The law specifies the components that these risk assessments and response plans must address, which include assessing the water system’s resilience and security of electronic and automated systems. However, SDWA section 1433 as amended by AWIA does not require EPA or authorized states to collect, review, or approve systems’ risk assessments or response plans, nor does it require the emergency response plans be submitted to EPA or be implemented by the systems. EPA issued guidance directly to water systems, developed a method for systems to certify that they had completed their assessment and plans, and tracked compliance.

Clean Water Act. The Clean Water Act, as amended, prohibits discharging certain pollutants into waters of the United States without a permit issued under the National Pollutant Discharge Elimination System.¹¹ Wastewater treatment facilities that discharge treated effluent—that is, sewage that has been treated to remove suspended solids and pollutants—into the waters of the U.S. are required to obtain such permits that limit discharges. Unlike drinking water systems regulated under SDWA, as amended by AWIA, the Clean Water Act does not have any comparable requirements for wastewater systems to assess their cybersecurity resilience and risk of cyberattack or develop emergency response plans.

Critical Infrastructure Roles and Responsibilities

The nation’s critical infrastructure refers to the systems and assets, whether physical or virtual, that are so vital to the U.S. that the incapacity or destruction of them would have a debilitating impact on U.S. security, economic stability, public health or safety, or any combination of these factors.¹²

Protecting the cybersecurity of critical infrastructure has been part of GAO’s High Risk List since 2003.¹³ In September 2018, we issued an update to the High Risk List that identified actions that federal agencies

¹⁰AWIA amended SDWA to require each community water system serving a population of greater than 3,300 “persons” to assess the risks to, and resilience of, its system. America’s Water Infrastructure Act of 2018, Pub. L. No. 115-270, § 2013, 132 Stat. 3765, 3850 (amending the Safe Drinking Water Act § 1433, 42 U.S.C. § 300i-2). SDWA defines “person” as an individual, corporation, company, association, partnership, state, municipality, or federal agency. 42 U.S.C. § 300(f)(12). EPA describes AWIA’s amendments to SDWA section 1433 as applying to each community water system serving more than 3,300 “people.”

¹¹Federal Water Pollution Control Act of 1972, Pub. L. No. 92-500, 86 Stat. 816 (1972) (amended and acknowledged as the “Clean Water Act” in Pub. L. No. 95-217, 91 Stat. 1566 (1977); codified at 33 U.S.C. §§ 1251-1387). See also 33 U.S.C. §§ 1311(a), 1342.

¹²42 U.S.C. § 5195c(e). The term “critical infrastructure” is defined in the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)*. Pub. L. No. 107-56, § 1016(e), 115 Stat. 272, 401.

¹³We first designated information security as a government-wide high-risk area in 1997. In 2003, we expanded this area to include cyber critical infrastructure protection. See GAO, *High-Risk Series: Efforts Made to Achieve Progress Need to Be Maintained and Expanded to Fully Address All Areas*, [GAO-23-106203](#) (Washington, D.C.: Apr. 20, 2023).

needed to take to address cybersecurity challenges that the nation faces.¹⁴ We later identified ensuring the nation's cybersecurity as one of nine high-risk areas that need especially focused executive and congressional attention.¹⁵ We continue to identify the cybersecurity of critical infrastructure as a component of the cybersecurity high-risk area, as reflected in our high-risk updates on major cybersecurity challenges.¹⁶ We have also previously reported on federal efforts to adopt the NIST cybersecurity framework and made related recommendations.¹⁷

Federal law and presidential policy designated EPA the Sector Risk Management Agency for the water sector, one of 16 critical infrastructure sectors.¹⁸ Various national-level plans and strategies also provide guidance and direction for the Sector Risk Management Agencies. These policies, plans, and laws include the following:

Presidential Policy Directive-21 (PPD-21). PPD-21, issued in February 2013, shifted the focus from protecting critical infrastructure against terrorism to protecting and securing critical infrastructure and increasing its resilience against all hazards, including cyber incidents. It made EPA responsible for leading, facilitating, and supporting the security and resilience programs and associated activities of the water sector in an all-hazards environment (including cyber incidents, natural disasters, terrorism, or other destructive criminal activity that targets critical infrastructure) in coordination with DHS, among other duties. DHS is to coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure.¹⁹ Further, PPD-21 also required DHS to update the National Infrastructure Protection Plan to articulate how this policy directive is to be implemented.

National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22). In April 2024, PPD-21 was rescinded and replaced by NSM-22, which established national principles and objectives related to strengthening U.S. critical infrastructure security and resilience.²⁰ These principles include advancing security and resilience through a risk-based approach, establishing and implementing minimum requirements for risk management, and leveraging expertise and technical resources from relevant federal departments and agencies to manage sector-specific risk. NSM-22 also reaffirmed the 16 critical infrastructure sector

¹⁴GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, [GAO-18-622](#) (Washington, D.C.: Sept. 6, 2018).

¹⁵GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: Mar. 6, 2019).

¹⁶GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021); *Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure*, [GAO-23-106441](#) (Washington, D.C.: Feb. 7, 2023).

¹⁷GAO, *Critical Infrastructure Protection; Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, [GAO-18-211](#) (Washington, D.C.: Feb. 15, 2018); *Critical Infrastructure Protection: Measures Needed to Assess Agencies' Promotion of the Cybersecurity Framework*, [GAO-16-152](#) (Washington, D.C.: Dec. 17, 2015); *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, [GAO-20-299](#) (Washington, D.C.: Feb. 25, 2020); and *Critical Infrastructure Protection: Agencies Need to Assess Adoption of Cybersecurity Guidance*, [GAO-22-105103](#) (Washington, D.C.: Feb. 9, 2022). As of February 2022, we reported that EPA had taken steps to determine the extent to which the water sector was implementing the cybersecurity framework.

¹⁸See 6 U.S.C. § 650(23). See also The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*.

¹⁹The White House, *Critical Infrastructure Security and Resilience*, Presidential Policy Directive-21 (Washington, D.C.: Feb. 12, 2013).

²⁰The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*.

designations and the Sector Risk Management Agencies for each sector. It established CISA as the National Coordinator for Security and Resilience of Critical Infrastructure and required the Secretary of Homeland Security to prepare a biennial National Infrastructure Risk Management Plan summarizing the U.S. government's efforts to assess and manage critical infrastructure risk. It also directs agencies to establish minimum security and resilience requirements within and across critical infrastructure, consistent with the 2023 National Cybersecurity Strategy (discussed below).

2013 National Infrastructure Protection Plan. Consistent with PPD-21, DHS updated its 2009 National Infrastructure Protection Plan to provide the overarching approach for integrating the nation's critical infrastructure protection and resilience activities into a single national effort.²¹ The 2013 National Infrastructure Protection Plan details federal roles and responsibilities in protecting the nation's critical infrastructure and how sector stakeholders should use risk management principles to prioritize protection activities within and across sectors. It emphasizes the importance of collaboration, partnerships, and voluntary information sharing among DHS; Sector Risk Management Agencies; industry owners and operators; and state, local, and tribal governments. Under this partnership, designated federal agencies serve as the lead coordinators for the security programs of their respective sectors.²²

Fiscal Year 2021 NDAA. This act amended the Homeland Security Act of 2002 to establish additional roles and responsibilities for designated agencies (i.e., Sector Risk Management Agencies) in securing critical infrastructure.²³ For example, the act requires designated agencies to provide specialized expertise, assess risks to the sector, and support risk management of their respective critical infrastructure sectors.

2023 National Cybersecurity Strategy. The strategy establishes five pillars and 27 strategic objectives for how the Office of the National Cyber Director will manage the nation's cybersecurity, particularly between the public and private sectors.²⁴ Pillar one, defend critical infrastructure, includes establishing cybersecurity requirements to support national security and public safety. The strategy states that the federal government will use existing authorities to set cybersecurity requirements and if there are gaps, the administration will work with Congress to close them.

Water and Wastewater Systems Face Increasing Cybersecurity Risk and Cyber Incidents

Threat actors, such as state-sponsored hackers or criminal groups, are increasingly capable of carrying out cyberattacks on water and wastewater systems. Increased connections between operational technologies and

²¹The Homeland Security Act of 2002, as amended, required DHS to develop a national plan for securing critical infrastructure, which it issued in 2006. PPD-21 directed DHS to update that national plan, which it issued in 2009 and 2013. See 6 U.S.C. § 652(e)(1)(E).

²²Department of Homeland Security, *NIPP [National Infrastructure Protection Plan] 2013*.

²³The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002, 134 Stat. 3388, 4768-73 (2021) (codified at 6 U.S.C. §§ 195f, 321m, 651-665d).

²⁴The White House, *National Cybersecurity Strategy*; and *National Cybersecurity Strategy Implementation Plan, Version 2* (Washington, D.C.: May 2024). The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 established the Office of the National Cyber Director within the Executive Office of the President. Pub. L. No. 116-283, § 1752, 134 Stat. 3388, 4144 (2021) (codified at 6 U.S.C. § 1500). The office is responsible for leading efforts to coordinate implementing the National Cybersecurity Strategy, among other actions. See GAO, *Cybersecurity: National Cyber Director Needs to Take Additional Actions to Implement an Effective Strategy*, [GAO-24-106916](#) (Washington, D.C.: Feb. 1, 2024).

internet-enabled devices, increased automation, and other factors have made water and wastewater systems more vulnerable to cyberattack. Although national-level reporting requirements for cyber incidents are under development, a number of known cybersecurity incidents in the U.S. over the past 5 years have disrupted water and wastewater system operations. Future incidents could have serious consequences.

Various Threat Actors Are Capable of Attacking Water and Wastewater Systems

A variety of threat actors can carry out cyberattacks on water and wastewater systems. These threat actors include nations, criminal groups, terrorists, and insiders (see table 1).

Table 1: Examples of Actors That Can Threaten Water and Wastewater System Cybersecurity

Threat actor	Description
Nations	Nations, including nation-state, state-sponsored, and state-sanctioned groups, or programs, use cyber tools as part of their information-gathering and espionage activities. These groups can also possess the ability to launch cyberattacks that can cause disruptive effects to critical infrastructure.
Criminal groups	Criminal groups, including organized crime organizations, seek to use cyberattacks for monetary gain. Criminal groups often use ransomware—malicious software used to deny access to IT systems or data—to hold systems or data hostage until a ransom is paid.
Terrorists and domestic violent extremists	Terrorists and domestic violent extremists seek to destroy, incapacitate, or exploit critical infrastructure to threaten national security, inflict mass casualties, weaken the economy, and damage public morale and confidence.
Hackers and Hacktivists	Hackers break into networks for a challenge, revenge, stalking, or monetary gain, among other reasons. Hacktivists are ideologically motivated and use cyber exploits to further political goals such as free speech or to make a point.
Insiders	Insiders are entities (e.g., employees, contractors, vendors) with authorized access to an information system or enterprise who have the potential to cause harm through destruction, disclosure, modification of data, or denial of service. Such destruction can occur wittingly or unwittingly.

Source: GAO analysis. | GAO-24-106744

The 2024 Annual Threat Assessment of the U.S. Intelligence Community stated that China, Iran, North Korea, and Russia posed the greatest cybersecurity threats to U.S. critical infrastructure.²⁵ The assessment stated that these countries possessed the ability to launch cyberattacks that could have disruptive effects on U.S. critical infrastructure.

Illustrating this threat, in February 2024, CISA, FBI, the National Security Agency, EPA, and other federal and international partners issued a joint advisory stating that Chinese-sponsored cyber actors from a group known as Volt Typhoon were seeking to pre-position themselves on IT networks to carry out cyberattacks in the event of a major crisis or conflict with the U.S.²⁶

²⁵Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 5, 2024).

²⁶Cybersecurity and Infrastructure Security Agency, *Cybersecurity Advisory: PRC [People’s Republic of China] State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, AA24-038A (February 2024). CISA and its U.S. and international partners previously issued an alert in May 2023 after detecting Volt Typhoon hacking into critical infrastructure in Guam, which is home to three American military bases. Microsoft, which first detected the hacking, noted that the operation’s likely aim was to disrupt critical communications between the U.S. and Asia region during a future crisis.

Cyberattacks That Move from IT to Operational Systems: Lateral Movement

Lateral movement is the process by which attackers spread from an entry point to the rest of the network. Attackers will typically gain initial entry to the target network, such as through a malware-infected computer connected to the network. Once the foothold is established, the attackers perform reconnaissance on the network and gain escalated use privileges until they can effectively access the entire network and the nodes connected to it.



Source: GAO (information); Gorodenkoff/stock.adobe.com (photo). | GAO-24-106744

Specifically, federal officials found that Volt Typhoon had compromised IT systems in the water sector and other critical infrastructure sectors, including energy, transportation, and communications. The alert stated that federal officials had a high degree of confidence that the attackers would be able to move from IT networks to operational technology assets and disrupt critical functions, such as supplying water or managing wastewater, a process known as lateral movement (see sidebar).

In addition, the FBI and other agencies reported in December 2023 that Iranian-affiliated attackers had hacked PLCs used in U.S. critical infrastructure—including water systems—by compromising default passwords on PLCs that were improperly accessible via the internet.²⁷ PLCs are used throughout the water sector (as well as in other industries such as power generation and manufacturing), and an attack on these devices can influence physical processes through the valves, motors, or pumps that are connected to the PLCs.

Insiders, such as current or former employees or contractors with remote access to operational systems, have also successfully carried out attacks against water and wastewater systems. For example, in March 2019, a former employee of a Kansas water district pleaded guilty to tampering with the water system by remotely accessing its cleaning and disinfecting processes with login credentials that had not been revoked after the employee left the organization.²⁸

Threat actors can use different techniques to gain access to water systems' IT or operational systems. These techniques include exploiting internet-accessible devices (such as the internet-exposed PLCs discussed

²⁷Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, *IRGC [Iranian Government Islamic Revolutionary Guard Corps]-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities*, AA23-335A (Dec. 1, 2023).

²⁸Press Release, Department of Justice, *Kansas Man Pleads Guilty to Water Facility Tampering* (Oct. 21, 2021). See also Indictment at 4, *United States v. Travnichek*, No. 5:21-cr-40029-TC (D. Kan. Mar. 31, 2021).

above), sending “spearphishing” emails with links or attachments that include malicious code, or exploiting services that allow users to connect to network resources from a remote location.

The public availability of cyberattack tools also means that attackers no longer need a great amount of skill to compromise business IT systems. Once an attacker has access to an IT system, the attacker can seek to steal data, degrade system performance, or provide access for future attacks. Threat actors may also become more capable over time, particularly with advances in artificial intelligence that could allow attackers to conduct cyberattacks faster and more effectively.²⁹ For more about the techniques that threat actors can use to gain access to water and wastewater IT and operational technology, see appendix II.

Water and Wastewater Systems Are Becoming More Vulnerable to Cyberattacks

A number of factors have made water and wastewater systems more vulnerable to cyberattack. These include increased connections between operational technologies and internet-enabled devices, increased automation and remote access capabilities, and operational and IT systems that are not properly separated by firewalls or other protections. For example, agency officials and industry representatives we interviewed said that operational technology in water and wastewater systems has become increasingly vulnerable to cyberattack. This increased vulnerability is because operational systems that once were largely isolated from the internet and business IT systems have become increasingly connected with those systems within and outside the organization. This convergence increases the ability of online attackers to reach these operational systems.

Additionally, water and wastewater system operators have reported automating water treatment and other functions to increase their systems’ efficiency, which sector officials told us is essential in areas where a single operator may have to run multiple small systems spread over a large geographic area. Similarly, adding remote access capabilities to treatment or pump operations allows operators to remotely respond to alarms or make adjustments to water processes—actions that previously had to be done manually. Vendors and other third-party contractors also rely on remote access to perform system maintenance and conduct updates to SCADA systems, PLCs, or other devices.

If water systems’ IT and operational systems are not properly separated using firewalls or other protections, cyberattacks that originate in business IT systems are more likely to migrate to operational systems and disrupt critical processes, as figure 5 shows.³⁰

²⁹According to the National Security Commission on Artificial Intelligence, the expanding application of existing artificial intelligence capabilities will make cyberattacks more precise and tailored, further accelerate and automate cyber warfare, enable stealthier and more persistent cyber weapons, and make cyber campaigns more effective on a larger scale. The National Security Commission on Artificial Intelligence, *Final Report* (March 2021).

³⁰A firewall is a device or program that controls the flow of network traffic between networks or hosts that employ different security postures.

Figure 5: Example of Water and Wastewater System Vulnerability to Cyberattack



Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/เทคทีทอนณ์ ทัฬหีฬ/James Thew/stock.adobe.com (photos). | GAO-24-106744

Accessible Text for Figure 5: Example of Water and Wastewater System Vulnerability to Cyberattack

- Water systems may contain hundreds of diverse components, making it difficult to properly map and keep operational technologies updated with security patches.
- Attackers may use IT networks to steal data or to move within the network to access operational systems.
- IT and operational networks may not be properly separated, allowing attackers to access the operational systems and disrupt critical processes.

Sources: Cybersecurity and Infrastructure Security Agency (information); ungvar/Rawpixel/James Thew/stock.adobe.com (photos). GAO-24-106744

In light of these increased cybersecurity threats and vulnerabilities, EPA stated in a May 2024 enforcement alert that it planned to increase its inspection and enforcement activity at drinking water systems.³¹ Specifically, EPA stated that it planned to increase the number of inspections that focused on cybersecurity, and where vulnerabilities are identified that may present an imminent and substantial danger to public health, enforcement actions may be appropriate to mitigate those risks.³²

³¹Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities* (May 20, 2024) (updated on June 1, 2024).

³²EPA has authority to issue enforcement orders and take other legal actions under SDWA. For example, when contamination or a potential terrorist or intentional attack on a public water system may present an imminent and substantial endangerment to public health, EPA can invoke emergency authority where appropriate. 42 U.S.C. § 300i.

Nevertheless, water and wastewater system operators have faced challenges with reducing their systems' vulnerability to cyberattacks. These challenges include addressing varying levels of cybersecurity capabilities and focus across the sector, managing workforce shortages, maintaining legacy systems that are difficult to update with cybersecurity protections, and prioritizing limited resources.

Addressing varying levels of cybersecurity capabilities and focus. EPA, CISA, and FBI reported in January 2024 that water and wastewater systems' varying levels of cybersecurity capabilities posed challenges to increasing cyber resilience across the sector. For example, CISA protective security advisors (PSA) and cybersecurity advisors (CSA) we interviewed stated that a lack of basic cyber hygiene—that is, actions to improve online security such as changing default passwords and keeping operating systems up to date—was a significant challenge for water and wastewater systems in their regions.

Further, industry officials we interviewed added that some water and wastewater system staff might be aware of cybersecurity as a general concern but might not dedicate significant time or effort to increasing their systems' capabilities to defend against cyberattacks. This lack of focus on cybersecurity comes, in part, from operators' belief that their system is unlikely to be targeted because it serves a small population or is located in a rural area. EPA recognized this challenge in a May 2024 enforcement alert, where it noted that small systems are not immune from cyberattacks.³³

Sector officials also reported that the water sector has lacked a focus on developing a cybersecurity culture—that is, a cyber risk management mindset among managers and staff combined with efforts to develop security awareness and vigilance. Specifically, a survey conducted by the Water Sector Coordinating Council in 2021 found that developing a cybersecurity culture was a major challenge for water and wastewater systems.³⁴ According to CISA, developing a cybersecurity culture can include practices such as providing regular training for staff on how to recognize phishing emails or developing policies and procedures to address changes in employee status, such as policies to revoke access credentials for former employees.³⁵

The *Roadmap to a Secure and Resilient Water and Wastewater Sector* also identified the need for the sector to develop a more robust cybersecurity culture at utilities of all sizes.³⁶ The roadmap, which was developed by a workgroup that included industry and government partners, established a near-term goal of maintaining and expanding a sector-wide focus on promoting basic cybersecurity practices, establishing cybersecurity policies, conducting cybersecurity training, and increasing user account security. For systems serving larger populations, the roadmap established a near-term goal of moving systems beyond minimum levels of cybersecurity.

³³Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*.

³⁴Water Sector Coordinating Council, *Water and Wastewater Systems: Cybersecurity: 2021 State of the Sector* (June 2021). The council collaborated on a survey to identify current cybersecurity practices in the sector and to better articulate the sector's challenges and needs. The voluntary survey was distributed to water and wastewater systems across the country by various national water and wastewater associations. The survey was conducted in April 2021 and resulted in 606 responses.

³⁵Cybersecurity and Infrastructure Security Agency, *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness* (2021).

³⁶Water and Wastewater Sector Strategic Roadmap Work Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*, EPA 810-R-24-002 (January 2024). The roadmap identified key vulnerabilities to the water sector such as supply chain risk management, extreme weather and natural disasters, physical and workforce safety, contamination incidents, infrastructure degradation, and cybersecurity and cyber risk management.

Managing workforce shortages. Water and wastewater systems, particularly smaller systems, face workforce shortages and other challenges. For example, a 2019 American Water Works Association report found that smaller systems often lacked enough staff with the time and knowledge needed to address cybersecurity issues.³⁷ Sector entities we interviewed reported that water and wastewater systems faced difficulties with hiring and retaining enough system operators, as well as planning for anticipated retirements.³⁸ These entities also reported that it was even more difficult to hire and retain staff with specialized cybersecurity experience and skills. While the largest and most technologically advanced water and wastewater systems may employ cybersecurity professionals, sector entities with whom we spoke said that small- and medium-sized systems generally do not because they reported being uncertain they needed such staff or were unable to provide competitive pay to recruit and retain staff. Water and wastewater systems therefore rely on operators with little or no cybersecurity expertise, or they outsource security to potentially expensive external contractors, according to officials we interviewed.

Maintaining legacy technologies. Sector entities we interviewed noted that water and wastewater systems tended to use older operational and IT systems that can be difficult to update as they age. Specifically, the nation's drinking water infrastructure includes more than 2.2 million miles of underground pipes and other related infrastructure that the American Society of Civil Engineers has said is aging and underfunded, with many older systems reaching the end of their design life.³⁹ Many of the operational technologies and IT software connected to this infrastructure are also reaching the end of their design lives. However, one official said that some of the older technologies, such as legacy control systems, are still reliable but not easy to change. Therefore, some operators prefer not to install updates that could disrupt their legacy technologies' performance and cause interruptions to operations.

In addition, many systems cannot go offline for extended periods for operators to make system updates because a continuous supply of water is important for health and sanitation, as well as for supporting other critical infrastructure such as health care and energy, according to sector officials. As a result, even in cases when technology providers distribute updates that include vital security fixes for identified vulnerabilities, water system operators may decide not to install the patches, therefore remaining vulnerable to attack. In other cases, officials told us that some operational technologies may be considered out of date and no longer supported by the original manufacturer, but because they continue to function and would be expensive to replace, the system operators continue using them.

Prioritizing limited resources. EPA and others have noted that water and wastewater systems must prioritize limited resources towards ensuring their ability to function—that is, to supply water and manage wastewater. As a result, government and sector officials have reported that the voluntary nature of cybersecurity competes with other regulated priorities, resulting in minimal or no cybersecurity investments.⁴⁰ Sector representatives with whom we spoke agreed that systems often have limited resources to meet multiple federal and state

³⁷Judith H. Germano, *Cybersecurity Risk and Responsibility in the Water Sector* (American Water Works Association, 2019).

³⁸In January 2018, we reported that the U.S. Bureau of Labor Statistics projected that 8.2 percent of existing water operators would need to be replaced annually between 2016 and 2026. GAO, *Water and Wastewater Workforce: Recruiting Approaches Helped Industry Hire Operators, but Additional EPA Guidance Could Help Identify Future Needs*, [GAO-18-102](#) (Washington, D.C.: Jan. 26, 2018).

³⁹American Society of Civil Engineers, *2021 Report Card on America's Infrastructure: Drinking Water* (2021).

⁴⁰Water and Wastewater Sector Strategic Work Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*.

requirements as well as meet maintenance demands to ensure consistent operations. These competing priorities for limited resources have resulted in cybersecurity being a lower funding priority.

For example, state and industry officials we interviewed said that water and wastewater systems have to comply with federal requirements under SDWA and Clean Water Act. Systems also have to make required (and often costly) infrastructure upgrades. These upgrades can include identifying and replacing lead pipes and preparing to manage emerging contaminants such as per- and polyfluoroalkyl substances (PFAS).⁴¹ Additionally, systems must also contend with the costs of routine maintenance on aging systems and budget funds for emergency repairs. Some officials told us that it can be difficult or impossible to expand their budgets for cybersecurity because their income is derived from rate-paying customers who may face financial hardship when rates increase. Declining populations may also make rate increases untenable for some systems.

Cyber Incidents Have Disrupted Some Water and Wastewater Operations, and Future Incidents Could Have More Significant Consequences

Cybersecurity incidents in the U.S. over the past 5 years have disrupted water and wastewater system operations.⁴² However, the full extent of such incidents and their consequences are unknown because national-level cybersecurity incident reporting requirements are under development, and water and wastewater systems have not yet been required to report incidents to the federal government. In addition, according to EPA officials, the national-level reporting requirements would exempt almost 80 percent of water and wastewater systems from reporting.⁴³

A 2021 joint cybersecurity advisory from CISA, FBI, the National Security Agency, and EPA detailed five known attacks on water and wastewater systems from 2019 through 2021.⁴⁴

⁴¹For example, by October 2024, drinking water systems must identify the materials of their service lines and notify individuals that are served by a line containing lead. 40 C.F.R. §§ 141.84(a), 141.85(e). Also, in December 2023, EPA issued a proposed rule that, among other things, would require 100 percent of lead service lines be replaced within 10 years. National Primary Drinking Water Regulations for Lead and Copper: Improvements (LCRI): Proposed Rule, 88 Fed. Reg. 84,878 (Dec. 6, 2023). Further, in April 2024, EPA issued a final rule that will require, among other things, water systems to reduce the level of six PFAS in drinking water. PFAS National Primary Drinking Water Regulation, 89 Fed. Reg. 32,523 (Apr. 26, 2024).

⁴²A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. See The White House, *Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination* (Washington, D.C.: July 26, 2016).

⁴³The Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires “covered entities” across critical infrastructure sectors to report “covered incidents” to CISA within 72 hours of reasonably determining a “covered incident” occurred. State, local, and municipal governments are not included as covered entities. CISA has 24 months from the date the act was signed into law to issue the proposed rule and an additional 18 months to issue a final rule. Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, div. Y (Cyber Incident Reporting for Critical Infrastructure Act of 2022), 136 Stat. 49, 1043 (2022) (codified at 6 U.S.C. § 681b). CISA published the draft rule in April 2024 with the final rule expected by August 2025. Cyber Incident Reporting for Critical Infrastructure Act (CIRICIA) Reporting Requirements, Proposed Rule, 89 Fed. Reg. 23,644 (Apr. 4, 2024).

⁴⁴Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Environmental Protection Agency, and National Security Agency, *Cybersecurity Advisory: Ongoing Cyber Threats to U.S. Water and Wastewater Systems*, AA21-287A (Oct. 14, 2021).

- An August 2021 ransomware attack on a California water and wastewater system. The ransomware variant had been in the system for about 1 month and was discovered when three SCADA servers displayed a ransomware message.
- A July 2021 ransomware attack on a Maine water and wastewater system's SCADA computer. The system was run manually until the SCADA computer was restored using local control.
- A March 2021 ransomware attack on a Nevada water and wastewater facility's SCADA system and backup systems.
- A September 2020 ransomware attack affecting files within a system at a New Jersey water and wastewater facility.
- A March 2019 attack at a Kansas facility where a former employee used unrevoked credentials to remotely access a facility computer and threatened drinking water safety.

Additionally, in November 2023, CISA and other sources reported that water and wastewater systems in multiple states experienced two types of cyberattacks. As discussed earlier, CISA, along with the FBI and other agencies, reported that the attackers likely accessed the PLCs by exploiting poor password security and the devices' exposure to the internet.⁴⁵ CISA added that the attackers had compromised PLCs in systems spanning multiple states but did not specify how many or which additional states. For example, media reports stated a Pennsylvania water system was the victim of foreign hackers that were targeting organizations using a specific brand of PLCs. The Pennsylvania water authority shut off the pumps that used the compromised PLCs and was able to maintain service by operating the pumps manually. Officials reported that there was no interruption or harm to the water supply.

Also in November 2023, a Texas water district reported a ransomware attack that affected business IT systems. The incident reportedly did not affect drinking water and wastewater operations, but officials reported that the telephone system was rendered temporarily unusable. A known ransomware group claimed responsibility for the attack.⁴⁶ The attackers posted evidence suggesting they had stolen sensitive data containing more than 33,000 files from the water district's systems.

In addition, some cybersecurity incidents that have affected water and wastewater systems have been the result of broader attacks targeting IT systems serving multiple municipal services, rather than a direct attack on the water or wastewater system. For example, in 2019, a major city experienced a ransomware attack against its municipal IT systems that, among other consequences, caused the city's department of public works to be unable to send bills to customers for several months.

Although there is not yet comprehensive data on cyber incidents affecting the water sector or consequences of these incidents, future incidents could have serious consequences. The FBI and others have reported that threat actors are becoming increasingly capable of conducting damaging cyberattacks. For example, in 2022, the FBI, CISA, and Department of the Treasury observed that several ransomware groups had developed code designed to stop critical infrastructure responsible for health care services, including electronic health records

⁴⁵Cybersecurity and Infrastructure Security Agency, *Cybersecurity Advisory: IRGC [Iranian Government Islamic Revolutionary Guard Corps]-Affiliated Cyber Actors*.

⁴⁶An October 2022 CISA joint cybersecurity advisory described the ransomware group as an active cybercriminal group targeting U.S. business in the public health and health care sector with ransomware and data extortion operations.

services, diagnostics services, and intranet services.⁴⁷ Further, we reported in January 2024 that the FBI had identified 870 critical infrastructure organizations that were victims of ransomware attacks in 2022, affecting nearly every critical infrastructure sector, including water.⁴⁸

EPA, CISA, and others have identified a range of potential cyberattack consequences, as table 2 describes.

Table 2: Potential Consequences of a Successful Cyberattack against Water and Wastewater Systems

Consequence	Description
Financial loss	Attackers may cause loss of productivity and revenue by damaging or disrupting the availability or integrity of water treatment processes. Further, paying the ransom associated with ransomware attacks can be costly yet may still not result in the system recovering its lost data. Attacks may also require systems to purchase new hardware or software.
Data loss or exposure	Attackers may gain access to databases of customer data held by water and wastewater systems or their municipal IT providers, including personal information and credit card details. Systems may also possess sensitive operational information that can be exploited.
Public health and environmental impact	Water and wastewater treatment relies on various chemicals throughout the treatment processes. These chemicals pose potential hazards, which, according to the Department of Homeland Security (DHS), vary depending on the volume, form, and concentration of the chemical if released. For example, chlorine gas (a commonly used disinfectant) is a respiratory irritant that may be fatal if inhaled or absorbed through skin. Drinking water contamination or wastewater degradation can be harmful to human, animal, and environmental health. For example, a wastewater service disruption can release hazardous chemicals into treated wastewater, negatively affecting public health and the environment. Contaminated drinking water can result in the need for individuals to access alternate water supplies or localities to issue public notices to boil water.
Loss of public trust or reputational damage	Due to water’s nature as a critical element for life, disruptions to the water supply may threaten a community’s stability and lead to decreased public confidence in the water supply. Service providers may also experience reputational damage following a cyberattack.
Cascading effects on other sectors and critical functions	Many other critical infrastructure sectors rely on water and wastewater for their operations. DHS reported that the loss of water and wastewater services would quickly cascade to energy, health care, communications, information technology, and emergency services, leading to the loss of critical services and negative effects on the economy, public health, and safety. For example, electric generation plants depend on water for steam generation, cooling, and fire suppression. Hospitals are also significantly dependent on water for core operations such as patient care, cooling, and hot water.

Source: GAO analysis of DHS, U.S. Environmental Protection Agency, and other information. | GAO-24-106744

Some, but not all, of these potential consequences can be mitigated by system operators. For example, on-site manual controls that override compromised automated systems could limit the severity of the consequences of a cyberattack, according to sector officials we interviewed. However, if a cyber incident results in multiple disruptions taking place simultaneously, such as over- or under-dosing chemicals or disrupting or disabling water flows, there might not be adequate staff to help manually mitigate these disruptions, according to DHS.⁴⁹

⁴⁷Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, Department of the Treasury, *Cybersecurity Advisory: North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector*, AA22-187A (July 7, 2022).

⁴⁸GAO, *Critical Infrastructure Protection, Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support*, GAO-24-106221 (Washington, D.C.: Jan. 30, 2024); Department of Justice, Federal Bureau of Investigation, Internet Crime Complaint Center, *Internet Crime Report, 2022*.

⁴⁹Department of Homeland Security, *Sector Resilience Report: Water and Wastewater Systems* (July 22, 2014).

System operators may also lack the training or skills needed to manually run a water system, according to officials. Specifically, operators may not have sufficient opportunities to practice running a system manually because shutting down automated systems to practice manual operations could disrupt water availability for customers.

Efforts to Improve Water Sector Cybersecurity Are Ongoing, but EPA Has Not Ensured a Key Risk Assessment Tool Produces Credible Results

Federal and non-federal entities have taken actions to improve water sector cybersecurity, including issuing alerts and advisories, conducting sector outreach and coordination, carrying out research and development, and distributing guidance and best practices. To help drinking water systems conduct risk and resilience assessments and develop emergency response plans, as required, EPA developed the Vulnerability Self-Assessment Tool (VSAT). However, EPA has not had VSAT peer reviewed to ensure the tool provides systems with sound and credible information.

Federal Agencies Have Shared Cybersecurity Alerts, Best Practices, and Other Guidance

EPA, CISA, and other federal agencies have taken actions to identify and share information on cybersecurity threats and responses.⁵⁰ For example, they have issued cybersecurity alerts and advisories, conducted sector outreach and coordination, carried out research and development, and distributed guidance and best practices.

Cybersecurity alerts and advisories. CISA and EPA disseminate regular cybersecurity alerts and advisories on their websites and through their email distribution lists. CISA generally develops these alerts and advisories, sometimes jointly with EPA and other federal agencies. Some alerts we reviewed were specific to a known cybersecurity vulnerability in a particular technology or software, such as the December 2023 cybersecurity advisory on the exploitation of PLCs in water and wastewater systems.⁵¹ Other alerts provided general guidance and suggested actions. For example, in February 2024, CISA issued a joint advisory with EPA and FBI on actions that water sector entities (such as system operators) can take to better protect water systems from malicious cyber activities.⁵² In May 2024, EPA also issued an enforcement alert that advised immediate steps that drinking water systems should take to reduce cybersecurity vulnerabilities.⁵³

⁵⁰Other federal agencies include the National Institute of Standards and Technology, the Federal Bureau of Investigation, and the Department of Homeland Security, as well as offices within agencies, such as DHS's Office of Intelligence and Analysis.

⁵¹Cybersecurity and Information Security Agency, *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems*, Cybersecurity Advisory, AA23-335A (Dec. 1, 2023).

⁵²Cybersecurity and Infrastructure Security Agency, *CISA, EPA, and FBI Top Cyber Actions for Securing Water Systems* (Feb. 23, 2024). The actions included changing default passwords, conducting regular cybersecurity assessments, and conducting cybersecurity awareness training.

⁵³Environmental Protection Agency, *Enforcement Alert: Drinking Water Systems to Address Cybersecurity Vulnerabilities*.

Because CISA's alerts cover a wide range of critical infrastructure sectors, EPA officials said they identify which of CISA's alerts are applicable to the water sector and share those alerts specifically with their water sector partners. EPA also reported working with sector organizations such as the American Water Works Association, Association of State Drinking Water Administrators, National Rural Water Association, Water Information Sharing and Analysis Center (WaterISAC), and others to encourage these organizations to share alerts and advisories with their members. CISA also works through the Joint Cyber Defense Collaborative to facilitate two-way information sharing with water and wastewater sector entities related to malicious activity and vulnerabilities.

Sector outreach and coordination. EPA and CISA conduct sector outreach through their websites and other means. For example, CISA has a webpage for water and wastewater cybersecurity that includes a toolkit of key resources for systems at every level of cybersecurity maturity, ranging from basic guidance for systems that are just starting to develop cybersecurity strategies to complex tools for more advanced systems. CISA's toolkit provides links to its free cybersecurity vulnerability scanning service for water systems, EPA's water resilience help desk, and EPA's free cybersecurity assessment services.⁵⁴ In addition, according to a DHS official, DHS's Office of Intelligence and Analysis offers access to the Homeland Security Information Network and fusion center staff to facilitate two-way threat intelligence sharing.

In addition, EPA and CISA's websites provide information on funding resources that water systems and states can use to make cybersecurity improvements. These funding sources include EPA's Clean Water and Drinking Water State Revolving Fund programs and CISA's State and Local Cybersecurity Grant Programs.⁵⁵

Also, CISA and EPA have made organizational changes to focus on cybersecurity and coordination. Specifically, CISA has a staff person (liaison) dedicated to water sector outreach and coordination. The liaison reported focusing on increasing CISA engagement with the water sector and conducting outreach at sector conferences and events. The liaison told us that these outreach efforts resulted in over 50 new water and wastewater systems enrolling in CISA's vulnerability scanning services—from 130 systems in December 2022 to 181 systems as of September 2023. In addition, EPA formed a branch office solely dedicated to cybersecurity by reallocating base levels of funding within its water security program, according to EPA officials.

⁵⁴Vulnerability scanning, which is available to all water and wastewater systems, provides systems with a weekly report that helps identify cybersecurity weaknesses that could be exploited by an attacker. These weaknesses include the presence of internet-accessible devices or vulnerabilities in a system's online assets that have already been targeted by threat actors and ransomware groups—referred to as known exploited vulnerabilities. CISA also provides best practices and guidance on stopping ransomware and recognizing and averting phishing attempts.

⁵⁵EPA awards grants to each state to establish a Clean Water State Revolving Fund, which states use to provide loans and other financial assistance to eligible recipients for the construction of municipal wastewater facilities, decentralized wastewater treatment systems, and other clean water projects. See 33 U.S.C. § 1383. Similarly, EPA awards grants to each state to establish a Drinking Water State Revolving Fund, which provides loans and other financial assistance for eligible water system infrastructure projects to improve drinking water treatment and water supply sources and other projects needed to protect public health and comply with SDWA. See 42 U.S.C. § 300j-12. The CISA State and Local Cybersecurity Grant Program provides grant funding to state, local, tribal, and territorial governments to address cybersecurity risks and threats to information systems owned and operated by, or on behalf of, these governments. See 6 U.S.C. § 665g.

Environmental Protection Agency's (EPA) Water Security Test Bed

EPA's water security test bed replicates a section of a typical municipal drinking water piping system. It allows EPA to test and evaluate technologies (such as sensors to detect contamination events) and processes (such as innovative water treatment processes) in an environment that simulates a typical operating water distribution system.



Source: EPA (information and photo). | GAO-24-106744

Research and development. EPA's Office of Research and Development plans to use its water security test bed at the U.S. Department of Energy's Idaho National Laboratory to research water system operational vulnerabilities to cyberattacks (see sidebar). EPA officials reported that the agency plans to use the test bed to examine SCADA vulnerabilities in water infrastructure, including how cyberattacks could affect system instrumentation, communications, or other computer-based controls. As of March 2024, EPA officials told us that research was in the planning phase because the cybersecurity portion of the water security test bed was currently under construction.

Additionally, in 2023, NIST's National Cybersecurity Center of Excellence initiated a project to outline common water and wastewater cybersecurity risk scenarios and desired security outcomes in areas such as remote access (e.g., eliminating shared and default accounts), asset management (e.g., creating an inventory of all network enabled devices), and network segmentation (i.e., ensuring IT and operational systems are appropriately separated). NIST officials told us in March 2024 that it has signed more than a dozen cooperative research and development agreements with technology vendors and water systems to carry out this work and plans to publish guidance on a rolling basis throughout fiscal years 2024 and 2025.⁵⁶

Guidance and best practices. EPA and CISA have developed and disseminated joint cybersecurity guidance and best practices for the water sector. For example, in January 2024, EPA, CISA, and the FBI issued a Water and Wastewater Sector Incident Response Guide.⁵⁷ This guide was designed to provide water sector owners and operators with information about federal roles, resources, and responsibilities for each stage of responding

⁵⁶NIST has also produced numerous guides and frameworks relevant to the water sector, including its Cybersecurity Framework, Guide to Operational Technology Security, and Security and Privacy Controls for Information and Organizations. See National Institute of Standards and Technology, *Cybersecurity for the Water and Wastewater Sector* (Washington, D.C.: June 2023); National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0* (Gaithersburg, Md.: February 2024); National Institute of Standards and Technology, *Guide to Operational Technology (OT) Security*; and National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Gaithersburg, Md.: September 2020).

⁵⁷Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and Environmental Protection Agency, *Incident Response Guide: Water and Wastewater Sector* (Washington, D.C.: January 2024).

to a cyber incident. In February 2024, CISA, EPA, and FBI issued a fact sheet on top cyber actions for securing water systems. The fact sheet included eight actions, such as conduct cybersecurity awareness training and develop incident response and recovery plans, with links to related EPA, CISA, and FBI resources. Additionally, in March 2024, CISA, EPA, and other federal and international partners issued an advisory on People's Republic of China state-sponsored cyber threats to the water, transportation systems, energy, and communications sectors.⁵⁸ The advisory suggested practices that sector leaders could take to increase supply chain security and develop a cybersecurity culture within their organizations.

Federal Agencies Provide Technical Assistance and Tools, but EPA Has Not Ensured Its Water Risk Assessment Tool Produces Credible Results

In addition to sharing information on cybersecurity threats and responses, federal agencies have provided technical assistance and tools, including training and exercises, to help water and wastewater systems identify and mitigate cybersecurity vulnerabilities.

CISA. CISA provides a range of virtual and in-person technical assistance and assessments, which it promotes through its website, working groups, and other forms of outreach. These include services, such as vulnerability scanning, that are available to all water and wastewater systems; assessments and services more applicable to advanced systems that have cybersecurity programs in place but are looking to further improve their security; and in-person technical assistance and assessments through CISA's regionally based PSAs and CSAs. CISA PSAs and CSAs are subject matter experts who assist critical infrastructure owners with assessments and resources to prepare for and respond to physical or cybersecurity incidents. For example, CISA's PSAs and CSAs conduct on-site physical and cybersecurity assessments for critical infrastructure owners and operators, including water and wastewater systems. These assessments include the Infrastructure Survey Tool, which helps systems identify their security measures and identify areas for improvement, and Cross-Sector Performance Goal assessments, which involve interview-based assessments of operational resilience and cybersecurity practices. Examples of voluntary assessments CISA has conducted for the water sector from fiscal years 2022 (when agency officials said the water sector became a priority sector for CISA) through 2023 are summarized in appendix III.

U.S. Department of Agriculture (USDA). USDA provides assistance that focuses specifically on small and rural systems. USDA administers the Circuit Rider Program, which includes a nationwide team of water professionals who provide training and technical assistance to water utility managers and other relevant sector partners. The program serves all 50 states and Puerto Rico and focuses on supporting small, rural water systems—that is, systems serving a population of 10,000 or fewer. While the Circuit Rider program typically supports rural systems with operational and other needs, officials and Circuit Riders with whom we met said that they have seen an increasing demand in recent years for cybersecurity support. USDA also administers the Technical Assistance and Training Grant Program, through which USDA officials said eligible nonprofit entities may provide technical assistance to rural water and wastewater systems related to cybersecurity.

⁵⁸The March 2024 advisory was issued jointly by CISA, EPA, FBI, the National Security Agency, the U.S. Department of Energy, U.S. Transportation Security Administration, and international partners. Specifically, the Australian Signals Directorate's Australian Cyber Security Centre, Canadian Communications Security Establishment's Canadian Center for Cyber Security, United Kingdom National Cyber Security Center, and New Zealand National Cyber Security Center contributed to the joint advisory.

EPA. EPA has provided technical assistance and tools, a dedicated cybersecurity webpage, training, and exercises. Specifically,

- **Water System Technical Assistance (WaterTA) programs.** These programs provide free support to communities for a range of water-related needs, including cybersecurity. As part of its WaterTA work, EPA developed a Water Cybersecurity Assessment Tool, which is a checklist of about 30 cybersecurity actions with related recommendations that, according to EPA officials, systems can complete on their own or with an EPA contractor. As of March 22, 2024, EPA reported that its contractor had provided cybersecurity assessments to 191 water or wastewater systems.⁵⁹
- **Dedicated webpage on cybersecurity.** EPA has centralized cybersecurity assessment and training resources on its website, which includes a variety of self-assessment resources (from EPA, CISA, NIST, and others). EPA also has a web form for water systems and other entities, such as state regulators, to request assistance directly from EPA through its Water Sector Cybersecurity Evaluation Program. From the beginning of fiscal year 2023 through February 2024, EPA reported that it has received 50 requests for assistance on a variety of cybersecurity topics. About half of the assistance requests (24 of 50) came from water systems (others were from state agencies or other assistance providers) and were for assistance on topics such as training, device and data security, and vulnerability management.

Safe Drinking Water Act (SDWA) Section 1433 Risk and Resilience Assessments

Certain drinking water systems serving more than 3,300 people are required to assess their vulnerability and resilience to cyberattacks, as well as to other malevolent acts, such as intentional contamination of finished water. Systems must also assess their risk from and resilience to natural hazards.

This and other information are used to inform emergency response plans.

Over 10,000 systems are subject to SDWA section 1433 assessment and planning requirements.



Source: Environmental Protection Agency and GAO analysis (information); tong2530/stock.adobe.com (photo). | GAO-24-106744

⁵⁹EPA developed the Water Cybersecurity Assessment Tool in 2023 to align with CISA's Cybersecurity Performance Goals. The Cybersecurity Performance Goals are a baseline set of cybersecurity practices and benchmarks for critical infrastructure operators to measure and improve their cybersecurity maturity in alignment with NIST's Cybersecurity Framework.

- **Training and exercises.** EPA reported that it has conducted 21 trainings with water and wastewater systems since fiscal year 2022. EPA reported that participants from over 3,000 systems have attended these trainings. Since March 2023, EPA has also offered Cybersecurity 101 and Cybersecurity Assessment training videos on its website. EPA has also provided an increasing number of cybersecurity exercises. Specifically, in fiscal year 2022, it offered one tabletop exercise with 45 participants.⁶⁰ In fiscal year 2023, that increased to 11 exercises with about 700 participants. As of February 2024, EPA had offered seven exercises to over 460 participants. Officials said they are working with CISA to identify locations where additional exercises would be beneficial.

In addition to these efforts, EPA developed a risk assessment tool—VSAT—to help drinking water systems that serve over 3,300 people to assess their vulnerability and resilience to cyberattacks and other threats (see sidebar).⁶¹ However, EPA has not taken key steps to ensure VSAT provides systems with sound and credible information to help them assess their cybersecurity risk. Specifically, EPA has not submitted VSAT for external peer review to ensure the assessment produces sound, credible risk results.

EPA guidance states that peer review is a documented process for enhancing a scientific or technical work product to help ensure that the decision or position that an agency takes, based on that product, has a sound, credible basis.⁶² Additionally, in a 2010 review of DHS’s approach to risk analysis, the National Research Council of the National Academies emphasized the importance of peer review as a strong scientific practice.⁶³ The National Academies noted that peer review is essential for developing guidelines around how risk information should be used, including how uncertainty in the risk estimates may affect the types of decisions that users make with the information.

⁶⁰According to EPA, a tabletop exercise is designed to test existing plans, policies, or procedures for guiding a response to a simulated incident. EPA facilitates exercises as well as provides information on its website for systems that want to design and run their own exercise.

⁶¹AWIA amended SDWA section 1433 to require each community water system serving a population of greater than 3,300 “persons” to assess the risks to, and resilience of, its system. 42 U.S.C. § 300i-2(a). EPA describes the requirement as applying to each community water system serving more than 3,300 “people.”

⁶²Environmental Protection Agency, Science and Technology Policy Council, *Peer Review Handbook*, 4th ed., EPA/100/B-15/001 (Washington, D.C.: October 2015).

⁶³The National Research Council of the National Academies, *Review of the Department of Homeland Security’s Approach to Risk Analysis* (Washington, D.C.: 2010).

Risks Can Be Assessed in Terms of Their Likelihood and Potential Consequences

Threat: a natural or man-made occurrence, individual, entity, or action that has the potential to harm life, information, operations, the environment, or property. In the case of intentionally adversarial actors, for both physical and cyber effects, the threat likelihood is estimated based on the intent and capability of the adversary.

Vulnerability: a physical feature or operational attribute that leaves an entity open to exploitation or susceptible to a given threat or hazard. A common measure of vulnerability is the likelihood that an attack is successful.

Consequence: the effect of an event, incident, or occurrence. Potential consequences may include public health and safety (e.g., loss of life and illness), economic (direct and indirect), psychological, and governance/mission impacts.



Source: Department of Homeland Security (information); กษัตริย์ สสมม /stock.adobe.com (photo). | GAO-24-106744

In March 2024, EPA officials said they had made updates to how VSAT calculates cybersecurity vulnerabilities and were making updates to how VSAT incorporates threat information, but they did not have plans to submit these updates for peer review.⁶⁴ Officials did not elaborate on why the agency was not planning to have these changes peer reviewed. However, they noted that one portion of VSAT—a calculator designed to help systems generate estimates of an incident’s consequences—underwent peer review in 2016. While reviewing individual elements of the model may be useful, a peer review of the entire VSAT model is still needed to determine that the results provided are sound and credible.

For example, a peer review could evaluate the appropriateness of VSAT’s method for integrating threat, vulnerability, and consequence values (see sidebar for definitions); the sufficiency of EPA’s documentation that details how the information water systems provide to VSAT is used to generate risk estimates; and the extent to which VSAT’s consequence estimates account for asset interdependencies, among other aspects of the model.

⁶⁴Specifically, officials told us they had integrated EPA’s Water Cybersecurity Assessment Tool checklist into VSAT so that if a system is implementing practices from the checklist, it reduces VSAT’s vulnerability score for the assets being evaluated. The Water Cybersecurity Assessment Tool is a checklist of approximately 30 practices and recommendations, such as changing default passwords and terminating individuals’ access to accounts or networks when warranted.

Additionally, a peer review could help EPA further align the model with the National Infrastructure Protection Plan's key principles for an effective risk assessment. These principles state that a risk assessment should be complete, documented, reproducible, and defensible. This includes documenting how information is integrated to generate risk estimates; communicating any uncertainty in the estimates; and producing comparable, repeatable results, even though infrastructure assessments may be performed by different analysts.

Taking action to ensure that VSAT is a high-quality risk assessment tool can provide EPA assurance that the risk and resilience assessments water systems conduct will provide useful information for response planning and other risk management efforts. While conducting a peer review requires an up-front commitment of time and resources, EPA's Peer Review Handbook states that the benefits usually justify these added resources. Submitting VSAT for peer review and making any necessary changes to the model can help EPA better ensure that the information water systems are producing is credible and helps them to appropriately identify and plan for cybersecurity risks.

States and Water Sector Groups Have Taken Action and Worked with Federal Partners to Address Cybersecurity Risks

States and water sector organizations have taken a range of actions and worked with federal partners to address cybersecurity risks to the sector. For example, in response to an October 2023 request from the Association of State Drinking Water Administrators, officials from 25 states voluntarily provided information on their state's approach to water sector cybersecurity. According to our review of this information, about one-third of the states reported they did not have a program in place but were actively considering ways to approach cybersecurity for their state's water systems. Other state officials reported sharing information and resources, as well as encouraging water systems to conduct cybersecurity assessments. Several states also reported partnering with CISA to identify resources and develop cybersecurity programs.

State drinking water and wastewater officials reported similar information in our interviews with them. For example, officials from two of five states told us that their states were developing or had already developed cybersecurity requirements using existing legal authorities or through statewide legislation. Conversely, officials from three of the five states we interviewed said their state did not have cybersecurity regulations or requirements for their water and wastewater systems. However, in one of these states, officials said they were working with regional CISA staff to develop a program to share cybersecurity information and to promote voluntary cybersecurity assessments for water systems. Officials added that they ultimately hoped to require systems to conduct cybersecurity assessments and that their state attorney general's office was evaluating whether existing legal authorities would allow the state drinking water agency to issue such requirements in the absence of a state law.

States and sector organizations have also worked with federal entities through various coordination groups as well as through information sharing and analysis centers. National water- and wastewater-related associations have also helped support the water sector with cybersecurity. This support has included developing and sharing information, including guidance and best practices; participating in sector-wide working groups; engaging in policy advocacy; and producing trainings and exercises. See appendix IV for additional information on these various efforts.

EPA Has Not Developed a Cybersecurity Strategy or Fully Evaluated Its Legal Authorities to Address Water Sector Risks

EPA has not conducted a comprehensive sector-wide risk assessment of the water sector's cybersecurity risk or used a risk-informed strategy to guide its actions, which our past work has shown is a basic underpinning for better managing federal programs and activities. Additionally, EPA's efforts to ensure water and wastewater systems take action to improve their cybersecurity have been met with legal and other challenges from the water sector. However, EPA has not fully evaluated the sufficiency of its existing legal authorities for achieving widespread implementation of key cybersecurity requirements for water and wastewater systems or taken action to identify and address any gaps in its authority.

EPA Has Not Comprehensively Assessed Sector Risk or Developed a Strategy to Guide Its Cybersecurity Efforts

EPA has not conducted a comprehensive sector-wide risk assessment or used a risk-informed strategy to guide its actions to improve the water sector's level of cybersecurity. We previously found that using a risk-informed strategy can improve the effectiveness of agency efforts to develop critical infrastructure cybersecurity programs.⁶⁵ The key characteristics of an effective strategy include the following:

- **Risk assessment.** Assesses the risks to critical assets and operations. We have also previously highlighted the importance of performing a cybersecurity risk assessment to help inform the steps that agencies should take when developing a critical infrastructure cybersecurity program.⁶⁶
- **Objectives, activities, and performance measures.** Addresses what the strategy is trying to achieve; steps to achieve those results; and the priorities, milestones, and performance measures that include measurable targets to gauge results and help ensure accountability. At the highest level, this could be a description of an ideal end state, followed by a logical hierarchy of major goals, subordinate objectives, and specific activities to achieve results. When defining the steps to achieve results, we have previously highlighted the importance of agencies determining whether they should act in a regulatory or advisory role.⁶⁷ We have also previously highlighted the importance of relying on NIST cybersecurity guidance to identify practices that critical infrastructure owners and operations should follow.⁶⁸
- **Roles, responsibilities, and mechanisms to coordinate efforts.** Addresses who will implement the strategy, what their roles will be, and mechanisms to coordinate their efforts. This characteristic entails identifying the specific federal departments, agencies, or offices involved, and, where appropriate, the

⁶⁵See, e.g., [GAO-23-105789](#). We have also reported that national strategies differ from other federal planning documents such as agency-specific strategic plans that the Government Performance and Results Act of 1993 requires. These strategies are national in scope, cutting across levels of government and sectors and involving a large number of organizations and entities (i.e., federal, state, local, and private sectors). [GAO-04-408T](#).

⁶⁶See, e.g., [GAO-19-332](#), [GAO-18-62](#), and [GAO-23-105789](#).

⁶⁷See, e.g., GAO, *Regulatory Guidance Processes: Selected Departments Could Strengthen Internal Control and Dissemination Practices*, [GAO-15-368](#) (Washington, D.C.: Apr. 16, 2015).

⁶⁸See, e.g., [GAO-19-332](#); [GAO-19-48](#); National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.1 (Apr. 16, 2018); and *Guide to Operational Technology (OT) Security*.

different non-federal (e.g., state, local, or private) entities. A strategy should clarify the organization's relationships in terms of leading, supporting, or sharing responsibilities. A strategy should also identify specific processes for coordination and collaboration between responsible entities.

- **Identification of needed resources and investments.** Addresses what the strategy will cost, the sources and types of resources and investments needed, and where those resources and investments should be targeted based on balancing risk reductions with costs. Specifically, a national strategy should elaborate on the risk assessment mentioned earlier and give guidance to implementing parties to manage their resources and investments accordingly.

However, EPA has not conducted a comprehensive sector-wide risk assessment or developed a risk-informed strategy for its water sector cybersecurity efforts. For example,

Risk Assessment. Risk assessment is a key characteristic of a successful national strategy. Sector Risk Management Agencies have been required by law to assess sector risk since 2021.⁶⁹ As the Sector Risk Management Agency for the water sector, EPA is required under the Fiscal Year 2021 NDAA to identify, assess, and prioritize water sector risk, including cybersecurity threats, vulnerabilities, and consequences.⁷⁰ The April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) also states that risk assessments must consider all threats and hazards, likelihoods, vulnerabilities, and consequences, as well as the scope and scale of dependencies within and across critical infrastructure sectors.⁷¹ It further states that Sector Risk Management Agencies should identify, assess, and prioritize sector-specific risk and support cross-sector and national risk assessment efforts. Last, it directs EPA to develop and biennially update a risk management plan that is informed by a sector-specific risk assessment.⁷²

EPA has assessed different aspects of cybersecurity risk. In particular, EPA developed threat information, analyzed cyber incidents to identify countermeasures, and convened workgroups with the water sector to develop reports to prioritize and mitigate risks. For example, EPA developed and updated the Baseline

⁶⁹6 U.S.C. § 665d(c)(2). Presidential Policy Directive-21 identified four areas of responsibility for Sector Risk Management Agencies—serving as the federal interface for prioritizing and coordinating sector-specific responsibilities; carrying out incident management responsibilities; providing, supporting, or facilitating technical assistance and consultations; and sharing information to support the DHS Secretary. The Fiscal Year 2021 NDAA expanded these responsibilities and added two new responsibilities. In addition to risk assessment, the other new responsibility identified in the Fiscal Year 2021 NDAA is for Sector Risk Management Agencies to contribute to emergency preparedness efforts, which is outside the scope of this review.

⁷⁰In addition to the Fiscal Year 2021 NDAA's risk assessment requirements, which include evaluating all potential risks, Executive Order 14110, *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, requires Sector Risk Management Agencies, including EPA, to specifically evaluate and provide annually to the Secretary of Homeland Security an assessment of the potential risks of artificial intelligence in the water sector—including how artificial intelligence makes the sector more vulnerable to critical failures, physical attacks, and cyberattacks—and consider potential mitigation measures that could address those vulnerabilities. Exec. Order 14,100, 88 Fed. Reg. 75,191 (Nov. 1, 2023). In response, EPA issued a non-public report in January 2024.

⁷¹The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*.

⁷²Specifically, within 180 days of the date of the National Security Memorandum (Apr. 30, 2024), Sector Risk Management Agencies shall develop plans to execute the required roles and responsibilities of each Sector Risk Management Agency to ensure a continuity of effort and the coordination of policy and resourcing requirements. Within 270 days and on a recurring basis biennial by February 1 of each year, each Sector Risk Management Agency shall submit its sector-specific risk management plan to the Secretary of Homeland Security, based on guidance developed by the Department of Homeland Security, through their Secretary or Agency Head. The plan shall be informed by the sector-specific risk assessment included as an annex. The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*.

Malevolent Threat for Community Water Systems document describing the likelihood of potential malevolent acts against water systems.⁷³

However, EPA officials said the agency has not conducted a sector-wide risk assessment. Specifically, a senior EPA official told us in May 2023 that EPA has considered threats, vulnerabilities, and consequences independently through various efforts, such as the voluntary vulnerability assessments it conducts for water and wastewater systems, but it has not integrated this information into a comprehensive sector-wide risk assessment.

Our past work has emphasized the integration of risk information in a comprehensive risk assessment.⁷⁴ For example, we reported in March 2009 that DHS's Transportation Security Administration—the lead federal agency for security in the transportation sector—had collected information related to threats, vulnerabilities, and consequences, but had not integrated these elements to assess risk for individual transportation modes (e.g., aviation, mass transit, pipelines) or to assess risk for the sector as a whole.⁷⁵ We reported that identifying and prioritizing risk in this way is essential to allocating resources towards the highest priority risks. Additionally, the 2013 National Infrastructure Protection Plan, which was developed to guide national efforts to manage risks to critical infrastructure, states that agencies should combine threat, vulnerability, and consequence information to inform a risk management approach.⁷⁶

EPA officials pointed to the risk and resilience assessments that community water systems conduct under SDWA section 1433, as amended by AWIA, as how EPA is supporting sector-wide risk assessment activities. However, this assessment requirement only applies to drinking water systems serving more than 3,300 people and does not apply to wastewater systems. Furthermore, according to EPA officials, EPA receives anonymized results of these assessments and reviews these assessments as part of drinking water system inspections, but does not approve the assessments or response plans.⁷⁷ Therefore, these assessments may help provide some information to understand drinking water system risk, but are not comprehensive enough to help EPA develop or inform a national-level, sector-wide risk assessment.

Objectives, activities, and performance measures. EPA has not identified cybersecurity-related goals, objectives, activities, and performance measures. Broadly, agency officials stated that the FY 2024-2027 National Enforcement and Compliance Initiative has an objective to achieve 100 percent compliance with the

⁷³Environmental Protection Agency, *Baseline Information on Malevolent Acts for Community Water Systems*, Version 3.0 (May 2024). EPA issued the first version in 2019.

⁷⁴GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, [GAO-23-105806](#) (Washington, D.C.: Feb. 7, 2023).

⁷⁵GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help TSA Inform Resource Allocation*, [GAO-09-492](#) (Washington, D.C.: Mar. 27, 2009).

⁷⁶Department of Homeland Security, *NIPP [National Infrastructure Protection Plan] 2013*.

⁷⁷SDWA section 1433, as amended by AWIA, does not require EPA or authorized states to collect, review, or approve drinking water systems' risk assessments or emergency response plans. America's Water Infrastructure Act of 2018, Pub. L. No. 115-270, § 2013, 132 Stat. 3765, 3850 (2018) (amending the Safe Drinking Water Act § 1433, 42 U.S.C. § 300i-2). EPA noted that it has reviewed assessments and response plan as part of its on-site compliance inspections under its SDWA section 1445 authority. See 42 U.S.C. § 300j-4(b)(1). Although EPA also has authority to request and collect these assessments and response plans, EPA officials stated that taking possession of the documents outside enforcement context puts the documents at risk of release under the Freedom of Information Act.

risk assessment and emergency response plans required under SDWA section 1433. However, EPA has not identified cybersecurity goals or objectives; how its activities help achieve those objectives; or the priorities, milestones, and performance measures needed to gauge results. When asked about cybersecurity goals for the sector, EPA officials said the agency wants to see 100 percent of water and wastewater systems with certain technologies (e.g., SCADA or a remote monitoring system) have a cybersecurity program in place. However, EPA has not identified those systems, prioritized steps for achieving a 100 percent goal, or identified milestones it hopes to achieve to gauge progress towards that goal.

Regarding performance measures, EPA officials said they look at rates of community water system compliance with SDWA section 1433's risk and resilience assessment requirement as a measure of sector performance. However, this measure only covers drinking water systems serving over 3,300 people and does not include wastewater systems. Officials said the agency also evaluates its performance by tracking the number of systems completing cybersecurity assessments, such as EPA's Water Cybersecurity Assessment Tool, or participating in EPA training and exercises. However, the agency has not established specific goals for (1) how many systems (or which systems) should participate in assessments, trainings, or exercises; or (2) the priorities, milestones, and performance measures it would need to gauge the results of its training or other efforts.

Roles, responsibilities, and mechanisms to coordinate efforts. EPA has not identified key roles and responsibilities or how efforts across the sector should be coordinated. EPA shares cybersecurity responsibilities with CISA and other government agencies but has not formally established roles and responsibilities for key activities. For example, a senior CISA official responsible for coordinating cybersecurity activities with EPA said that EPA has not communicated its priorities or how efforts should be coordinated across the many varied sector entities (e.g., states and municipalities with water oversight responsibilities, sector associations, or other federal partners).

In addition, a January 2024 report from the DHS Office of Inspector General also found that CISA had not collaborated with EPA to integrate CISA's cybersecurity expertise with EPA's water expertise.⁷⁸ The Inspector General recommended that CISA establish and implement a written memorandum of understanding with EPA to fully document each agency's roles and responsibilities and mechanisms for collaboration, which CISA agreed to do by the end of calendar year 2024.

Identification of needed resources and investments. EPA's resource requests have not been linked to risk-informed goals. We have previously emphasized the importance of using risk information to inform resource decisions. EPA reported that its appropriated funding for its Sector Risk Management Agency duties, including its cybersecurity responsibilities, was \$11.8 million in fiscal year 2023. EPA has made budget requests for additional cybersecurity staff, funding to start a grant program, and funding to carry out cybersecurity incident preparation, response, and recovery work; however, the requested funding amounts have not been

⁷⁸U.S. Department of Homeland Security, Office of Inspector General, *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector*, OIG-24-09 (Washington, D.C.: Jan. 9, 2024).

appropriated.⁷⁹ Developing risk-informed goals and linking its funding requests to those goals could help EPA better demonstrate how its budget priorities are appropriately informed by risk.

In lieu of a sector-wide strategy, EPA reported relying on the risk assessments and response plans required under SDWA section 1433 and various documents to serve as guiding principles for its water sector cybersecurity efforts. These documents include the 2022 *Prioritization Framework for Technical Cybersecurity Support to Public Water Systems*, a 2021 national security memorandum on control system cybersecurity and the sector-developed the 2024 *Roadmap to a Secure and Resilient Water and Wastewater Sector*.⁸⁰ These documents and the risk assessments and response plans discuss challenges that the sector faces, but they do not address the key characteristics of a national water sector strategy.

While these documents assess aspects of risk for the sector, they do not assess sector-wide risk, define specific risk-reduction objectives, or define how EPA's activities align to those objectives. For example, these documents do not define how EPA will measure its progress towards achieving specific cybersecurity goals, such as how many systems (and which types of systems) EPA wants to see develop cybersecurity programs by certain dates. Further, the documents do not establish sector-wide roles and responsibilities or how sector entities will coordinate their efforts. The documents also do not identify needed resources and investments to achieve specific sector-wide cybersecurity goals.

Our past work has shown that assessing risk and having a risk-informed strategy is a basic underpinning for better managing federal programs and activities.⁸¹ A sector-wide risk assessment could help EPA identify the highest risks that its programs should address and prioritize actions to address those risks. Incorporating such information into a national strategy could help EPA more effectively allocate its resources and support requests for any additional resources it needs to carry out its cybersecurity programs. In addition, since numerous federal and nonfederal agencies share responsibility for managing the sector's cybersecurity risk, a strategy could help EPA establish clear roles and responsibilities for carrying out programs and activities. A clearly articulated strategy can also enhance agency officials' and congressional decision-makers' ability to ensure accountability and provide oversight. Without a sector-wide risk assessment and risk-informed strategy to guide its cybersecurity efforts, EPA has limited assurance that its actions and its resources are addressing the highest cybersecurity risks.

⁷⁹Specifically, EPA officials told us that in its fiscal years 2023 and 2024 budgets, the agency requested about \$4 million and an additional six full time equivalent staff to support its cybersecurity work, which to date has not been appropriated. For fiscal years 2023, 2024, and 2025, EPA also requested \$25 million to establish a cybersecurity grant program that would provide funding directly to water systems (rather than through states). According to EPA officials, the grant program funding has not been appropriated to date. In fiscal year 2024, EPA also requested \$19.6 million to carry out its cybersecurity programs and increase the agency's ability to respond to incidents.

⁸⁰Environmental Protection Agency, *Prioritization Framework for Technical Cybersecurity to Public Water Systems – Report to Congress*, EPA817-R-22-001 (May 2022); The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (Washington, D.C.: July 28, 2021); and Water and Wastewater Sector Strategic Roadmap Work Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*.

⁸¹[GAO-04-408T](#); [GAO-17-300](#); [GAO-19-332](#); [GAO-23-105789](#); and GAO, *Environmental Liabilities: DOE Would Benefit from Incorporating Risk-Informed Decision-Making into Its Cleanup Policy*, [GAO-19-339](#) (Washington, D.C.: Sept. 18, 2019).

EPA Has Not Fully Evaluated Its Approach to Using Its Legal Authorities to Reduce Water Sector Cybersecurity Risks

EPA's efforts to ensure water and wastewater systems take action to improve their cybersecurity have faced legal and other challenges from the water sector. As the Sector Risk Management Agency for water and wastewater, EPA is required to establish and carry out programs to assist the water sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to water systems, including cybersecurity risks.⁸² However, EPA has faced challenges using both its existing legal authority and voluntary approaches to encourage sector action. These challenges have contributed to the sector's minimal rate of progress, according to EPA officials and cybersecurity analysts.

EPA has evaluated some aspects of its existing legal authorities and its approach to managing the sector's cybersecurity risks. EPA's current approach to managing the water sector's cybersecurity risks stems from EPA's 2014 response to Executive Order 13636, Improving Critical Infrastructure Cybersecurity.⁸³ As directed, EPA assessed its existing legal authorities in 2014 and determined that they were sufficient to establish cybersecurity requirements for drinking water and wastewater systems, but decided to pursue voluntary approaches at that time.⁸⁴

However, over the last decade, EPA has faced challenges using both its existing legal authority as well as voluntary approaches to ensure water and wastewater systems are taking action to improve their cybersecurity. For example, in March 2023, EPA interpreted existing legal requirements—rather than issuing a new regulation—to require states to assess cybersecurity at drinking water systems. However, it suspended this effort 7 months later following legal challenges. Specifically, several states challenged EPA's memorandum that interpreted SDWA regulations to require primacy states (i.e., states that are approved to implement the federal drinking water program) to conduct cybersecurity assessments for drinking water systems during on-site reviews called sanitary surveys.⁸⁵ The states alleged EPA exceeded its legal authority in its interpretation that the sanitary survey requirements must include a cybersecurity evaluation.⁸⁶ In October 2023, EPA withdrew the memorandum, but encouraged all states to voluntarily engage in reviewing public water system cybersecurity programs through the sanitary survey or an alternate process.⁸⁷

⁸²6 U.S.C. § 665d(c)(1).

⁸³Exec. Order No. 13636, 78 Fed. Reg. 11,739, 11,743-44 (Feb. 19, 2013).

⁸⁴In May 2014, EPA stated that it reported to the President on February 7, 2014, that EPA had the authority to establish cybersecurity requirements for public (drinking) water systems under SDWA section 1401 and for publicly owned treatment works (wastewater systems) under the Clean Water Act sections 304, 308, 402, and 501.

⁸⁵Environmental Protection Agency, *Addressing Public Water System Cybersecurity in Sanitary Surveys or an Alternate Process* (Mar. 3, 2023). Primacy states are required to conduct periodic on-site reviews (called sanitary surveys) of public water systems to evaluate whether the water system facilities, equipment, operation, and maintenance are adequate for producing and distributing safe drinking water. 40 C.F.R. §§ 141.2, 142.16(b)(3), 142.16(o)(2).

⁸⁶Petition for Review, *Missouri v. EPA*, No. 23-1787 (8th Cir. Apr. 17, 2023). The American Water Works Association and National Rural Water Association joined the litigation, stating that EPA's interpretative memorandum imposed new administrative and financial burdens on their members and the systems that would be subject to the new interpretation. In July 2023, the court stayed the memorandum, pending the outcome of litigation.

⁸⁷Environmental Protection Agency, *Withdrawal of Cybersecurity Memorandum of March 3, 2023* (Oct. 11, 2023).

EPA has also faced challenges using voluntary approaches to ensure the sector is implementing cybersecurity practices. For example, it has stated that it cannot develop cybersecurity performance metrics because of sector resistance to voluntarily providing baseline information. Specifically, in response to a November 2015 GAO recommendation that EPA develop performance metrics to provide data and determine how to overcome challenges to monitoring water and wastewater systems' cybersecurity progress, EPA officials stated that water sector associations and water system owners and operators had affirmed their opposition to voluntarily developing and collecting cybersecurity metrics.⁸⁸ These officials said in December 2023 that the agency therefore had no viable route by which to acquire data and develop water-specific performance metrics.

Since EPA last assessed its existing legal authorities in 2014 and determined that a voluntary approach to implementing cybersecurity practices was sufficient, the water sector has faced increasing risk. EPA's responsibilities as the Sector Risk Management Agency for the water sector have also increased.⁸⁹ EPA stated in 2014 that if the voluntary partnership model was not successful in achieving widespread implementation of key cybersecurity practices, or if changing cybersecurity risks warranted, it could revisit the option of using its general statutory authority under SDWA and Clean Water Act to establish cybersecurity requirements. Yet, to date, EPA has not assessed whether its voluntary partnership model has been successful in managing cybersecurity risks and any changes to those risks. According to EPA's written comments, the agency had conducted a thorough examination of its authorities; however, as of July 2024, we were not provided documentation of EPA's evaluation of its authorities under SDWA and the Clean Water Act.

EPA officials said in March 2024 that the agency did not have express legal authority to issue cybersecurity requirements, but continued to believe it had sufficient legal authority under SDWA and Clean Water Act to issue regulations using its rulemaking process. Officials also said that the agency was continuing to evaluate the scope of its authorities, including whether existing requirements could be interpreted to include cybersecurity. Officials told us that they have sought additional authorities from Congress to ensure drinking water utilities are better protected from cyberattacks. However, EPA did not have plans to evaluate whether it needed to work with the administration and Congress for additional or clarified legal authorities to carry out its cybersecurity responsibilities considering recent litigation challenging EPA's authority. It is also unclear whether EPA has evaluated its authorities to address challenges related to collecting and protecting information and data from water systems' assessments of cybersecurity risks.

The White House's NSM-22, issued April 2024, directs regulatory and oversight entities to establish and implement minimum requirements to address sector-specific and cross-sector cybersecurity risks. It further requires federal agencies like EPA to use regulations, drawing on existing voluntary consensus standards as appropriate, to establish minimum requirements and effective accountability mechanisms to ensure the security and resilience of critical infrastructure. Further, the 2023 National Cybersecurity Strategy also directs federal agencies to use existing authorities to set necessary cybersecurity requirements. However, if agencies have gaps in their statutory authorities to implement minimum cybersecurity requirements, the strategy states that the administration will work with Congress to close those gaps.⁹⁰ Given the water sector's changing risk environment and EPA's new requirements under NSM-22, fully evaluating the sufficiency of its existing legal

⁸⁸GAO, *Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress*, [GAO-16-79](#) (Washington, D.C.: Nov. 19, 2015).

⁸⁹[GAO-23-105806](#).

⁹⁰The White House, *National Cybersecurity Strategy*.

authorities for managing cybersecurity risks and working with the administration and Congress to close any gaps could help EPA ensure the water sector is better prepared for any future cyberattacks.

Conclusions

The water sector faces an increasing array of cybersecurity risks, as well as significant challenges to addressing those risks. EPA, as the Sector Risk Management Agency, has provided cybersecurity resources, including training, guidance, voluntary assessments, and other programs. However, the agency has not taken key steps that would help it target its efforts and more effectively address cybersecurity risk.

First, EPA has not conducted a comprehensive sector-wide risk assessment, as required by law, or used a risk-informed strategy to guide its cybersecurity efforts across the water sector. For a sector as large and decentralized as the water sector, a risk-informed national strategy is important for identifying and prioritizing assets; establishing roles and responsibilities; justifying and targeting resources; and developing performance measures. Without a comprehensive sector-wide risk assessment and a risk-informed national cybersecurity strategy, EPA has limited assurance that its programs and resources are most effectively addressing the water sector's significant and increasing cybersecurity risk.

Second, EPA has faced challenges using both its existing legal authority and voluntary approaches to improve the sector's level of cybersecurity but has not fully evaluated the sufficiency of its existing legal authorities for the water sector since 2014. Evaluating the sufficiency of EPA's existing legal authorities and working with the administration and Congress to close any gaps could help ensure the water sector is better prepared for any future cyberattacks.

Lastly, EPA has not submitted its risk assessment tool, VSAT, for external peer review, as called for in EPA guidance. By doing so and making revisions to the tool, as appropriate, EPA would better ensure the tool produces reliable information that helps water systems appropriately identify and prepare for the highest cybersecurity risks to their systems.

Recommendations for Executive Action

We are making a total of four recommendations to EPA:

The Administrator of EPA should, as required by law, conduct a water sector risk assessment, considering physical security and cybersecurity threats, vulnerabilities, and consequences. (Recommendation 1)

The Administrator of EPA should develop and implement a risk-informed cybersecurity strategy, in coordination with other federal and sector stakeholders, to guide its water sector cybersecurity programs. Such a strategy should include information from a risk assessment and should identify objectives, activities, and performance measures; roles, responsibilities, and coordination; and needed resources and investments. (Recommendation 2)

The Administrator of EPA should evaluate its existing legal authorities for carrying out EPA's cybersecurity responsibilities and seek any needed enhancements to such authorities from the administration and Congress. (Recommendation 3)

The Administrator of EPA should submit the Vulnerability Self-Assessment Tool (VSAT) for independent peer review and revise the tool as appropriate. (Recommendation 4)

Agency Comments

We provided a draft of this report for review and comment to EPA, DHS, and the Departments of Justice, Commerce, and Agriculture (USDA). EPA provided written comments, reproduced in appendix V. EPA, DHS, and FBI provided technical comments, which we incorporated as appropriate. Commerce and USDA did not provide comments.

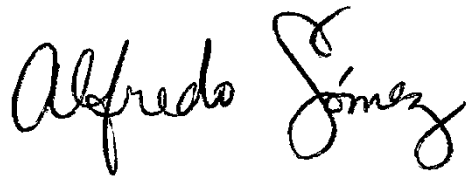
In its written comments, EPA concurred with all four of our recommendations and indicated that it would complete a water sector risk assessment and risk management plan by January 2025. EPA also stated that its Water Sector Cybersecurity Task Force would continue to build upon the 2024 *Roadmap to a Secure and Resilient Water and Wastewater Sector* to develop risk-informed recommendations of actions to improve the cybersecurity state of practice in the water sector.

In addition, EPA estimated that the peer review of VSAT would begin in November 2024, and, if necessary, a revised VSAT would be published in August 2025.

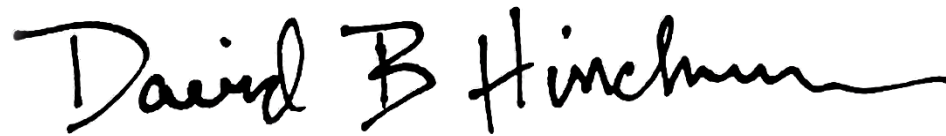
Although EPA concurred with our third recommendation, it stated that it had already conducted a thorough examination of, and provided technical assistance to Congress on, existing legal authorities for drinking water systems with respect to its cybersecurity responsibility. Further, the agency committed to providing a detailed explanation of its examination of legal authorities as part of the risk management plan, to be completed in 2025. Until this explanation is completed and available, however, we are unable to assess the degree to which EPA has examined its legal authorities. Specifically, we cannot assess the extent to which the examination addresses EPA's authority related to wastewater systems or the collection and protection of data and information on water systems' assessments of cybersecurity risks. In addition, over the last decade, EPA has faced challenges using its existing legal authority as well as voluntary approaches to ensure water and wastewater systems are taking actions to improve their cybersecurity. Consequently, we still believe that further evaluation of EPA's legal authorities is necessary because the current approach to managing the water sector's cybersecurity risks stems from EPA's 2014 assessment.

We are sending copies of this report to appropriate congressional committees; the Environmental Protection Agency; the Departments of Agriculture, Commerce, Homeland Security, and Justice; and other interested parties. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or staff members have any questions about this report, please contact J. Alfredo Gómez at (202) 512-3841 or gomezj@gao.gov, and David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VI.

A handwritten signature in black ink that reads "Alfredo Gómez". The signature is written in a cursive style with a large, stylized 'A' and 'G'.

J. Alfredo Gómez
Director, Natural Resources and Environment

A handwritten signature in black ink that reads "David B. Hinchman". The signature is written in a cursive style with a large, stylized 'D' and 'H'.

David B. Hinchman
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

This report (1) describes cybersecurity risks and water sector incidents, (2) examines actions selected federal and nonfederal entities have taken to improve water sector cybersecurity, and (3) evaluates the extent to which the Environmental Protection Agency (EPA) has taken actions to address known cybersecurity risks to the water sector.

To address all three of our objectives, we analyzed documentation from relevant federal and state agencies, visited one drinking water and two wastewater systems that were selected to provide perspectives from large and small systems, interviewed federal- and state-level officials, and obtained the perspectives of nonfederal organizations and sector associations representing various aspects of the water sector.

Federal agencies. We interviewed officials from five federal agencies with responsibilities related to water sector oversight, cybersecurity, or critical infrastructure protection. Specifically, we interviewed officials from the EPA's Office of Water, Office of Research and Development, and Office of Homeland Security; the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA); the Department of Commerce's National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence; the U.S. Department of Agriculture's (USDA) Rural Development office; and the Department of Justice's Federal Bureau of Investigation (FBI).

Within CISA, we interviewed a nongeneralizable sample of regional cybersecurity advisors (CSA) and protective security advisors (PSA) in five regions, covering 21 states, five territories, and the District of Columbia to discuss their perspectives on cybersecurity challenges that water systems face and how systems are using federal resources to address those challenges.¹ We selected PSAs and CSAs from CISA regions that included states CISA identified in a 2021 cybersecurity advisory as having experienced cyberattacks on their water and wastewater systems from 2019 through 2021. Those states were California, Kansas, Maine, and Nevada. We also interviewed the CSA and PSA from the CISA region that includes Maryland, because of Maryland's experience managing a 2019 cyber incident that affected a major city's water utility billing system.

State agencies. We interviewed a nongeneralizable sample of officials with water sector oversight responsibilities from five state environmental or public health-related agencies. Specifically, we interviewed state officials responsible for drinking water in Maine and Maryland and interviewed officials from state agencies responsible for both drinking water and wastewater in California, Kansas, and Nevada. We selected four of five states (California, Kansas, Maine, New Jersey, and Nevada) that CISA identified in its 2021 cybersecurity advisory as having experienced cyberattacks on their water and wastewater systems from 2019 through 2021.² We also selected a fifth state, Maryland, because of its experience managing a 2019 cyber

¹CSAs offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial officials, among other duties. PSAs offer cybersecurity assistance to critical infrastructure owners and operators and state, local, tribal, and territorial officials, among other duties. We interviewed a CSA in CISA Region 2 (New Jersey, New York, Puerto Rico, and U.S. Virgin Islands); and a CSA and PSA in Region 1 (Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont); Region 3 (Delaware, District of Columbia, Maryland, Pennsylvania, Virginia, and West Virginia); Region 7 (Iowa, Kansas, Missouri, and Nebraska); and Region 9 (Arizona, California, Hawaii, Nevada, Guam, American Samoa, and Commonwealth of the Northern Mariana Islands).

²CISA's memo also identified New Jersey; however, New Jersey officials did not respond to our requests for an interview.

incident that affected a major city's water utility billing system. Information from our interviews with state agencies cannot be generalized to all states but provided us with information specific to how those states were addressing water sector cybersecurity issues.

Water and wastewater systems. We also toured drinking water and wastewater treatment plants and interviewed water and wastewater operators in Maryland and the surrounding area. Specifically, we interviewed system operators and toured the facilities of three systems—Brunswick Water Treatment Plant and Conococheague Wastewater Treatment Plant in Maryland, and Blue Plains Advanced Wastewater Treatment Plant in Washington, D.C. We met with local officials and drinking water system operators in Middletown, Maryland, but did not tour the water facility. We also interviewed officials from American Water, a private water and wastewater company serving 14 million customers in 24 states. We selected these systems to provide the perspectives of both large and small systems, as well as urban and rural systems. The information we obtained in these visits is not generalizable to all water or wastewater systems but provided us with an overview of IT and operational technology at facilities of different sizes and serving differently sized populations.

Nonfederal organizations and sector associations. We interviewed officials from the Water Information Sharing and Analysis Center (WaterISAC), which was established in 2002 and is the designated information sharing and operations arm of the Water Sector Coordinating Council.³ We also interviewed officials from the Multi-State Information Sharing and Analysis Center, which is responsible for improving state, local, tribal, and territorial government cybersecurity through information sharing and other means.

We interviewed officials from seven national water sector associations. They were the American Water Works Association, the Water Environment Foundation, the National Association of Clean Water Agencies, Association of State Drinking Water Administrators, Association of Clean Water Administrators, Association of Metropolitan Water Agencies, and the National Rural Water Association. These national water associations represent drinking water, wastewater, urban and rural systems, and state water and wastewater administrators. We selected these organizations because of their relevant knowledge of water and wastewater systems, state regulatory requirements, challenges facing systems of all sizes and types, and for their knowledge of water sector cybersecurity.

Within the National Rural Water Association, we interviewed state-level staff called Circuit Riders, who provide services to rural water and wastewater systems under a contract with USDA. We interviewed Circuit Riders in California, Kansas, Maine, New Jersey, and Nevada—i.e., the same states where CISA had identified water systems that had experienced cyber incidents. We interviewed Circuit Riders to better understand the challenges facing small, rural systems.

To describe cybersecurity risks and water sector incidents, we reviewed relevant publicly available reports on threats and cybersecurity incidents, as well as EPA, CISA, and other federal guidance and advisories. We also

³The Water Sector Coordinating Council serves as a policy, strategy, and coordination body that works with EPA, DHS, and other federal agencies on matters of critical infrastructure security and resilience. Membership includes the American Water Works Association, Association of Metropolitan Water Agencies, National Rural Water Association, and other national water associations.

reviewed our prior reports on cybersecurity threats to critical infrastructure.⁴ In addition, we interviewed the above listed federal and non-federal officials to discuss cybersecurity threats, vulnerabilities, and potential consequences.

To examine actions selected federal and nonfederal entities have taken to improve water sector cybersecurity, we reviewed relevant documentation of information sharing, technical assistance, guidance, training, and research and development taken by those entities. We also evaluated the extent to which EPA's Vulnerability-Self Assessment Tool (VSAT) can help community (drinking) water systems serving more than 3,300 people to develop risk and resilience assessments, as required by America's Water Infrastructure Act of 2018 (AWIA).⁵ We reviewed available documentation on VSAT, which we compared with the risk assessment standards in the 2013 National Infrastructure Protection Plan and its supplemental risk management tool, and to the standards set forth in EPA's Peer Review Handbook.⁶ The National Infrastructure Protection Plan states that a risk assessment should be,

- Documented (i.e., clearly document what information is used and how it is synthesized to generate a risk estimate).
- Complete (i.e., should assess consequence, vulnerability, and threat for every defined risk scenario).
- Reproducible (i.e., should produce comparable, repeatable results and minimize the number and impact of subjective judgements).
- Defensible (i.e., must logically integrate its components, communicate any uncertainty associated with consequence estimates, and communicate the level of confidence in the vulnerability and threat estimates).

Last, we interviewed the above-listed federal and nonfederal officials to discuss steps entities have taken to improve water sector cybersecurity.

To evaluate the extent to which EPA has taken actions to address known cybersecurity risks to the water sector, we reviewed documentation on actions that EPA had taken to identify and respond to cybersecurity risks. These documents included EPA memoranda, advisories, and planning documents. We also interviewed officials from EPA regarding agency actions to address cybersecurity risks. We compared EPA's actions with the Sector Risk Management Agency requirements in the Homeland Security Act of 2002, as amended by the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Fiscal Year 2021 NDAA), the critical infrastructure protection priorities in the 2023 National Cybersecurity Strategy, the sector risk assessment standards in the 2013 National Infrastructure Protection Plan, and GAO criteria for developing

⁴For example, see GAO, *Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid*, [GAO-19-332](#) (Washington, D.C.: Aug. 26, 2019); *Electric Grid Cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems*, [GAO-21-81](#) (Washington, D.C.: Mar. 18, 2021); *Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure*, [GAO-23-105789](#) (Washington, D.C.: Oct. 26, 2022); *Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management*, [GAO-19-48](#) (Washington, D.C.: Dec. 18, 2018); and *Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods*, [GAO-23-105468](#) (Washington, D.C.: Sept. 26, 2023).

⁵America's Water Infrastructure Act of 2018, Pub. L. No. 115-270, § 2013, 132 Stat. 3765, 3850 (amending the Safe Drinking Water Act § 1433, 42 U.S.C. § 300i-2).

⁶Department of Homeland Security, *National Infrastructure Protection Plan, Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach* (2013); and Environmental Protection Agency, Science and Technology Policy Council, *Peer Review Handbook*, 4th ed., EPA/100/B-15/001 (Washington, D.C.: October 2015).

and implementing effective program strategies.⁷ We also reviewed the updated Sector Risk Management Agency requirements in the April 2024 National Security Memorandum on Critical Infrastructure Security and Resilience.⁸

We conducted this performance audit from April 2023 through July 2024, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁷The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 9002(c)(1), 134 Stat. 3388, 4770-72 (2021) (amending the Homeland Security Act of 2002) (codified at 6 U.S.C. § 665d); The White House, *National Cybersecurity Strategy* (March 2023); Department of Homeland Security, *NIPP [National Infrastructure Protection Plan] 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013); GAO, *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism*, [GAO-04-408T](#) (Washington, D.C.: Feb. 3, 2004); and [GAO-23-105789](#).

⁸The White House, *National Security Memorandum on Critical Infrastructure Security and Resilience*, National Security Memorandum 22 (Washington, D.C.: Apr. 30, 2024).

Appendix II: Cyber Threat Techniques

Threat actors can use a variety of techniques to compromise target systems. For examples of common techniques attackers could use, see table 3.

Table 3: Potential Techniques Available to Cyber Attackers

Threat type	Description
Ransomware	Ransomware is a form of malicious software designed to encrypt files on a device, rendering any data and systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. The ransomware perpetrators can assert that the system or encrypted data will remain unavailable, be deleted, or released publicly if the ransom is not met. Alternatively, the perpetrators can assert that if the ransom is paid, the victim will receive the information needed to regain access to the system or unencrypt the data.
Viruses and worms	A program that “infects” computer files, usually via executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Viruses require human interaction to propagate, while worms do not.
Spearphishing	Spearphishing attacks target specific individuals using spoofed emails or similar tactics to deliver malicious payloads. Spearphishing is the most prevalent method used by advanced persistent threat actors to deliver payloads.
Watering hole attacks	Watering hole attacks involve attackers compromising legitimate websites used by their target, such as the website for a trade organization or for technical information. Attackers typically infect the targeted website with malware intended to collect information and credentials entered by users on the site. Attackers can then use gathered credentials to gain access to target systems.
Supply chain compromise	Attackers may compromise the supply chain of information technology and operational technology products by manipulating hardware or software products, or the delivery mechanisms of products before receipt by the end consumer.
Remote login exploits	Attackers may exploit services that allow users to connect to network resources from a remote location. The attackers then use these services to access and attack network technologies.

Source: GAO. | GAO-24-106744

Appendix III: Examples and Reported Numbers of Cybersecurity and Infrastructure Security Agency Security Assessments

The Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) reported conducting a range of cybersecurity and physical security assessments for critical infrastructure owners and operators. CISA-reported examples of selected assessments conducted for the water sector (e.g., drinking water and wastewater systems) and other critical infrastructure sectors are summarized in table 4.

Table 4: Examples of Cybersecurity and Infrastructure Security Agency (CISA) Security Assessments and Reported Numbers of Assessments Conducted for the Water Sector and All Other Sectors, Fiscal Years (FY) 2022 and 2023

Assessment	Description and level	Who conducts them	Number conducted for the water sector – FY 2022	Number conducted for all other sectors – FY 2022	Number conducted for the water sector – FY 2023	Number conducted for all other sectors – FY 2023
Infrastructure Survey Tool	Web-based assessment to identify and document the overall physical security and resilience of a facility. Intermediate	Regional protective security advisors	35	218	41	461
Cyber Infrastructure Survey	Evaluates effectiveness of organizational security controls, cybersecurity preparedness, and overall cybersecurity resilience. Foundational	Regional cybersecurity advisors	23	91	29	275
Cyber Resilience Review	Interview-based assessment that evaluates operational resilience and cybersecurity practices. Advanced	Regional CSAs	34	158	30	210
Remote penetration testing	Simulates the tactics and techniques of real-world adversaries to identify and validate a perimeter’s exploitable pathways. Intermediate	CISA’s Cybersecurity Division	13	195	16	193
Risk and Vulnerability Assessment	Simulates tactics and techniques of real-world adversaries to identify and validate exploitable pathways on external and internal networks. Intermediate	CISA’s Cybersecurity Division	31	124	10	155

Appendix III: Examples and Reported Numbers of Cybersecurity and Infrastructure Security Agency Security Assessments

Assessment	Description and level	Who conducts them	Number conducted for the water sector – FY 2022	Number conducted for all other sectors – FY 2022	Number conducted for the water sector – FY 2023	Number conducted for all other sectors – FY 2023
Web application scanning	Evaluates publicly accessible websites for potential bugs and weak configurations to provide recommendations for mitigating web application security risks. Foundational	CISA's Cybersecurity Division	52	1,249	52	1,529
Vulnerability scanning	Evaluates external network presence by scanning public, static internet protocol addresses for accessible services and vulnerabilities. Provides weekly vulnerability reports and ad hoc alerts. Foundational	CISA's Cybersecurity Division	133	4,210	191	6,090
Validated architecture design reviews	Assists with architecture and design review, system configuration, and other system elements. Intermediate/advanced	CISA's Cybersecurity Division	4	18	7	16

Source: GAO analysis of CISA information. | GAO-24-106744

Note: "Foundational" refers to services and resources that are available and recommended to all users, regardless of capability. "Intermediate" are services that require users to have some experience developing and implementing security policies and procedures either on their own or through previous CISA engagements. "Advanced" are services that, because of their expansive scope and technical complexity, require preexisting capabilities and programs already in place within an organization that can be leveraged as prerequisites for receiving that service.

"All other sectors" refers to the 15 sectors other than the Water and Wastewater Systems Sector.

Appendix IV: Actions Taken by State and Water Sector Organizations to Address Cybersecurity Risks

States and water sector organizations have taken a range of actions and worked with federal partners to address cybersecurity risks to the sector. For example, some states have reported sharing information and conducting assessments, while others reported that they are investigating how they will approach cybersecurity for their water and wastewater systems. Specifically, in response to an October 2023 request from the Association of State Drinking Water Administrators, officials from 25 states voluntarily provided information on their state's approach to water sector cybersecurity. About half of the states reported they did not have a program in place but were actively considering ways to approach cybersecurity for their state's water systems. Other state officials reported sharing information and resources, as well as encouraging water systems to conduct cybersecurity assessments. Several states also reported partnering with CISA to identify resources and develop cybersecurity programs.

State drinking water and wastewater officials reported similar information in our interviews with them. For example, officials from two of five states told us that their states were developing or had already developed cybersecurity requirements using existing legal authorities or through state-wide legislation. Officials from one state said that their agency had authority to collect information from water and wastewater systems and that their agency was working with CISA to develop a cybersecurity assessment program. Officials from another state told us that a 2022 state law required certain water and wastewater systems to develop cybersecurity plans and complete vulnerability assessments, and to provide that information to the state.

Conversely, officials from three of the five states we interviewed said their state did not have cybersecurity regulations or requirements for their water and wastewater systems. However, in one of these states, officials said they were working with regional CISA staff to develop a program to share cybersecurity information with local governments as well as directly with water systems, and to promote voluntary cybersecurity assessments for water and wastewater systems. Officials added that they ultimately hoped to require systems to conduct cybersecurity assessments. Accordingly, officials said that the state attorney general's office was evaluating whether existing legal authorities would allow the state drinking water agency to issue such requirements in the absence of a state law.

States and sector organizations have also worked with federal entities through various coordination groups. For example, state, local, tribal, territorial, federal, and non-governmental entities collaborate through the Water Sector Government Coordinating Council and Sector Coordinating Council.¹ The Government Coordinating Council, of which EPA is chair, also includes other federal agencies, state departments of

¹The Government Coordinating Council provides interagency, intergovernmental, and cross-jurisdictional activity, strategy, and policy coordination on topics related to cybersecurity, infrastructure security, and water sector resilience. The Sector Coordinating Council serves as a policy, strategy, and coordination mechanism, comprised of water sector associations and system owners, that recommends actions to reduce and eliminate security and resilience vulnerability in the sector. The Sector Coordinating Council and Government Coordinating Council are partners in prioritizing, planning, coordinating, implementing, and executing sector-wide cybersecurity and resiliency efforts.

environmental management, state departments of health, and various national water associations. The Sector Coordinating Council comprises industry associations and water and wastewater system owners.

The councils have taken actions to identify the sector's cybersecurity challenges and needs. Most recently, in January 2024, the councils, in collaboration with EPA, CISA, and others, produced an updated *Roadmap to a Secure and Resilient Water and Wastewater Sector*, which discusses key threats and vulnerabilities to the sector and identifies near- and mid-term actions to address those gaps.² Additionally, in June 2021, the Sector Coordinating Council, in collaboration with industry and other sector entities, conducted a survey of U.S. water and wastewater systems to better understand the sector's cybersecurity challenges and needs.³ In the resulting report, the council identified federal and other resources that could help meet those needs, such as increased training and information sharing, as well as resource gaps.

States and sector organizations also participate in information sharing and analysis centers, which are member-supported organizations that deliver all-hazards threat and mitigation information to critical infrastructure asset owners and operators.

- **Multi-State Information Sharing and Analysis Center.** This center, which shares cybersecurity threat information, alerts, and guidance, includes over 15,000 members of state, local, tribal, and territorial government organizations and a number of federal agencies.
- **WaterISAC.** States and other sector partners—including several hundred water and wastewater system operators, government agencies, and private companies—also participate in or are members of the WaterISAC. WaterISAC hosts regular briefings on cybersecurity topics; provides resources on security threats; shares links to EPA, CISA, NIST, and other organizations' assessment tools and guidance; and shares quarterly summaries of incidents and suspicious activities at water and wastewater systems. In 2019, WaterISAC produced a list of 15 cybersecurity fundamentals.⁴

National water- and wastewater-related associations have also helped support the water sector with cybersecurity. This support has included developing and sharing information, including guidance and best practices; participating in sector-wide working groups; engaging in policy advocacy; and producing trainings and exercises. For example, the American Water Works Association, whose members include over 4,300 water and wastewater systems and other individuals involved in the water sector, provides cybersecurity risk management guidance, a cybersecurity assessment tool, and guidance specific to small systems.⁵ Other sector associations specifically support the needs of state agencies that oversee water and wastewater systems in their states. Specifically, the Association of State Drinking Water Administrators and the National

²Water and Wastewater Sector Strategic Roadmap Working Group, *Roadmap to a Secure and Resilient Water and Wastewater Sector*, EPA 810-R-24-002 (January 2024).

³Water Sector Coordinating Council, *Water and Wastewater Systems: Cybersecurity, 2021 State of the Sector* (June 2021).

⁴Water Information Sharing and Analysis Center, *15 Cybersecurity Fundamentals for Water and Wastewater Utilities: Best Practices to Reduce Exploitable Weaknesses and Attacks* (Washington, D.C.: 2019). WaterISAC requires a membership to access some of its information and services, and sector organization officials said that this was a challenge for some smaller systems that could not afford membership dues.

⁵American Water Works Association, *Water Sector Cybersecurity Risk Management Guidance, Version 3.0* (2019). American Water Works Association also provides an online risk and resilience training and certification for large and small systems, advocates nationally for water sector policies, and hosts a national conference that includes additional cybersecurity training and education opportunities for states, water system staff, and others. The association also shares guidance from EPA, CISA, NIST, and other agencies on its website.

Association of Clean Water Administrators participate in sector-wide working groups, share information at workshops and conferences, conduct research and advocacy, and share EPA and CISA guidance and tools with their members, among other actions.

Appendix V: Comments from the Environmental Protection Agency



OFFICE OF WATER
WASHINGTON, D.C. 20460

Mr. Alfredo Gomez
Director
Natural Resources and Environment
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Gomez:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's draft report, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems* (GAO-24-106744).

The purpose of this letter is to provide the U.S. Environmental Protection Agency's response to the draft report's findings, conclusions, and recommendations. The EPA agrees with the GAO's findings, conclusions, and recommendations and is providing responses to each recommendation.

Additionally, as an enclosure to this letter, the EPA is providing detailed technical comments on the information used to support the findings and inform GAO's recommendations. These technical comments clarify information, provide important context, and address technical or factual inaccuracies contained within the draft report.

The EPA has provided responses to the draft report's recommendations as follows:

GAO Recommendation 1

The Administrator of EPA should, as required by law, conduct a water sector risk assessment, considering physical security and cybersecurity threats, vulnerabilities, and consequences.

EPA Response

The EPA concurs with this recommendation. The EPA will develop a water sector risk assessment and risk management plan that addresses cybersecurity in accordance with the *National Security Memorandum on Critical Infrastructure Security and Resilience*, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

GAO Recommendation 2

The Administrator of EPA should develop and implement a risk-informed cybersecurity strategy, in coordination with other federal and sector stakeholders, to guide its water sector cybersecurity programs. Such a strategy should include information from a risk assessment and should identify objectives, activities, and performance measures; roles, responsibilities, and coordination; and needed resources and investments.

EPA Response

The EPA concurs with this recommendation. The EPA will develop a water sector risk assessment and risk management plan that addresses cybersecurity in accordance with the National Security Memorandum on Critical Infrastructure Security and Resilience, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

In addition, the EPA has convened a Water Sector Cybersecurity Task Force comprised of representatives from federal, state, and local levels, as well as water system participants and other sector stakeholders. This Task Force will continue to build upon the *2024 Roadmap to a Secure and Resilient Water and Wastewater Sector* to develop risk-informed recommendations of actions to improve the cybersecurity state of practice in the water sector.

GAO Recommendation 3

The Administrator of EPA should evaluate its existing legal authorities for carrying out EPA's cybersecurity responsibilities and seek any needed enhancements to such authorities from the administration and Congress.

EPA Response

The EPA concurs with this recommendation. The EPA has already conducted a thorough examination of and provided technical assistance to Congress on existing legal authorities with respect to our cybersecurity responsibility. In addition, the EPA will provide a detailed explanation of this examination as part of the water sector risk management plan being developed in support of the National Security Memorandum on Critical Infrastructure Security and Resilience, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

GAO Recommendation 4

The Administrator of EPA should submit the Vulnerability Self-Assessment Tool (VSAT) for independent peer review and revise the tool as appropriate.

EPA Response

The EPA concurs with this recommendation. The EPA will submit the Vulnerability Self-Assessment Tool for independent peer review and revise the tool as appropriate. The EPA estimates the peer review will begin in November 2024 and a revised VSAT, if necessary, will be published in August 2025.

Again, thank you for the opportunity to review and provide input on GAO's draft report. If you have any questions, please contact Colin Jones, OW's GAO Audit Follow-up Coordinator, at (202) 564-2959 or at Jones.Colin@epa.gov.

Sincerely,

For BENITA
BEST-WONG
Bruno Pigott
Acting Assistant Administrator

Digitally signed by
BENITA BEST-WONG
Date: 2024.07.10
16:52:30 -0400

ENCLOSURE

1. Technical Comments on GAO's draft report, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems* (GAO-24-106744)

cc: Benita Best-Wong, OW/IO
Nancy Grantham, OW/IO
Macara Lousberg, OW/IO/OPARMS
Janita Aguirre, OW/IO/OPARMS
Greg Spraul, OW/IO/OPARMS
Colin Jones, OW AFC
Carla Hagerman, OW AFC
Jennifer McLain, OW/OGWDW
Yu-Ting Guilaran, OW/OGWDW
Karen Wirth, OW/OGWDW
David Travers, OW/OGWDW
Brian Pickard, OW/OGWDW
Nushat Thomas, OW/OGWDW
Cecil Rodrigues, OECA/IO
Loan Nguyen, OECA AFC
Rosemarie Kelley, OECA/OCE
Jacqueline Werner, OECA/OC
Kathryn Caballero, OECA/FFEO
Kristien Knapp, OCIR
Michael Harris, OCIR
Stuart Miles-Mclean, OP
Joshua Florentino, OP
Sue Perkins, OCFO
Brittany Wilson, OCFO
Shay Bracey, OCFO

Accessible Text for Appendix V: Comments from the Environmental Protection Agency

Mr. Alfredo Gomez
Director
Natural Resources and Environment
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Gomez:

Thank you for the opportunity to review and comment on the U.S. Government Accountability Office's draft report, *Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems* (GAO-24-106744).

The purpose of this letter is to provide the U.S. Environmental Protection Agency's response to the draft report's findings, conclusions, and recommendations. The EPA agrees with the GAO's findings, conclusions, and recommendations and is providing responses to each recommendation.

Additionally, as an enclosure to this letter, the EPA is providing detailed technical comments on the information used to support the findings and inform GAO's recommendations. These technical comments clarify information, provide important context, and address technical or factual inaccuracies contained within the draft report.

The EPA has provided responses to the draft report's recommendations as follows:

GAO Recommendation 1

The Administrator of EPA should, as required by law, conduct a water sector risk assessment, considering physical security and cybersecurity threats, vulnerabilities, and consequences.

EPA Response

The EPA concurs with this recommendation. The EPA will develop a water sector risk assessment and risk management plan that addresses cybersecurity in accordance with the National Security Memorandum on Critical Infrastructure Security and Resilience, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

GAO Recommendation 2

The Administrator of EPA should develop and implement a risk-informed cybersecurity strategy, in coordination with other federal and sector stakeholders, to guide its water sector cybersecurity programs. Such a strategy should include information from a risk assessment and should identify objectives, activities, and performance measures; roles, responsibilities, and coordination; and needed resources and investments.

EPA Response

The EPA concurs with this recommendation. The EPA will develop a water sector risk assessment and risk

management plan that addresses cybersecurity in accordance with the National Security Memorandum on Critical Infrastructure Security and Resilience, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

In addition, the EPA has convened a Water Sector Cybersecurity Task Force comprised of representatives from federal, state, and local levels, as well as water system participants and other sector stakeholders. This Task Force will continue to build upon the 2024 Roadmap to a Secure and Resilient Water and Wastewater Sector to develop risk-informed recommendations of actions to improve the cybersecurity state of practice in the water sector.

GAO Recommendation 3

The Administrator of EPA should evaluate its existing legal authorities for carrying out EPA's cybersecurity responsibilities and seek any needed enhancements to such authorities from the administration and Congress.

EPA Response

The EPA concurs with this recommendation. The EPA has already conducted a thorough examination of and provided technical assistance to Congress on existing legal authorities with respect to our cybersecurity responsibility. In addition, the EPA will provide a detailed explanation of this examination as part of the water sector risk management plan being developed in support of the National Security Memorandum on Critical Infrastructure Security and Resilience, published on April 30, 2024. The water sector risk assessment and risk management plan will be completed in January 2025, and refreshed biannually thereafter.

GAO Recommendation 4

The Administrator of EPA should submit the Vulnerability Self-Assessment Tool (VSAT) for independent peer review and revise the tool as appropriate.

EPA Response

The EPA concurs with this recommendation. The EPA will submit the Vulnerability Self-Assessment Tool for independent peer review and revise the tool as appropriate. The EPA estimates the peer review will begin in November 2024 and a revised VSAT, if necessary, will be published in August 2025.

Again, thank you for the opportunity to review and provide input on GAO's draft report. If you have any questions, please contact Colin Jones, OW's GAO Audit Follow-up Coordinator, at (202) 564-2959 or at Jones.Colin@epa.gov.

Sincerely,

For BENITA BEST-WONG

Digitally signed by BENITA BEST-WONG

Date: 2024.07.10

16:52:30 -04'00'

Bruno Pigott

Acting Assistant Administrator

ENCLOSURE

1. Technical Comments on GAO's draft report, Critical Infrastructure Protection: EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems (GAO-24-106744)

cc: Benita Best-Wong, OW/IO

Nancy Grantham, OW/IO

Macara Lousberg, OW/IO/OPARMS

Janita Aguirre, OW/IO/OPARMS

Greg Spraul, OW/IO/OPARMS

Colin Jones, OW AFC

Carla Hagerman, OW AFC

Jennifer McLain, OW/OGWDW

Yu-Ting Guilaran, OW/OGWDW

Karen Wirth, OW/OGWDW

David Travers, OW/OGWDW

Brian Pickard, OW/OGWDW

Nushat Thomas, OW/OGWDW

Cecil Rodrigues, OECA/IO

Loan Nguyen, OECA AFC

Rosemarie Kelley, OECA/OCE

Jacqueline Werner, OECA/OC

Kathryn Caballero, OECA/FFEO

Kristien Knapp, OCIR

Michael Harris, OCIR

Stuart Miles-Mclean, OP

Joshua Florentino, OP

Sue Perkins, OCFO

Brittany Wilson, OCFO

Shay Bracey, OCFO

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

J. Alfredo Gómez at (202) 512-3841 or gomezj@gao.gov

David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Susan Iott (Assistant Director), Michael W. Gilmore (Assistant Director), Charlotte Gamble (Analyst in Charge), Ben Atwater, Mark Braza, Jillian Clouse, Tara Congdon, Crystal Huggins, Joseph Kirschbaum, Shep Ryen, India Sharpe, Sara Sullivan, Jason Trentacoste, Linda Tsang, and AJ Yohn made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Sarah Kaczmarek, Acting Managing Director, KaczmarekS@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548