Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems

November 13, 2024 | Report No. 25-N-0004

November 13, 2024

MEMORANDUM

SUBJECT: Management Implication Report: Cybersecurity Concerns Related to Drinking Water Systems

FROM: Nicolas Evans, Acting Assistant Inspector General
Office of Investigations

TO: Bruno Pigott, Principal Deputy Assistant Administrator
Office of Water

Purpose: The U.S. Environmental Protection Agency Office of Inspector General has identified cybersecurity concerns at drinking water systems. Additionally, the OIG has identified weaknesses with reporting and coordinating responses to potential cybersecurity incidents at these water systems. Drinking water systems are critical infrastructure. As such, identifying and addressing cybersecurity concerns within these systems and reporting and coordinating responses to potential cybersecurity incidents is critical to preventing related disruption, corruption, and dysfunction, and to protecting public health. We conducted this investigation in accordance with the *Quality Standards for Investigations* published in November 2011 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we conduct investigations in a timely, efficient, thorough, and objective manner.

Background: The Safe Drinking Water Act, or SDWA, is a foundational piece of environmental law aimed at protecting public health by creating standards for our nation's drinking water systems. To this end, SDWA authorizes the EPA to set health-based drinking water standards to protect against both naturally occurring and synthetic contaminants. These standards apply to all public water systems in the United States and ensure that the water provided to consumers is safe to drink.

A key feature of SDWA is the delegation of primary implementation and enforcement responsibility, also known as "primacy," to states, territories, and tribes. The EPA can delegate this authority for public drinking water systems to states, territories, and tribes that meet certain requirements, such as adopting regulations that are at least as stringent as federal standards, maintaining an inventory of public water systems, and having adequate enforcement capabilities. Currently, all but one state, all territories, and the Navajo Nation are primacy agencies. The EPA retains overall responsibility for the national implementation of SDWA and oversees SDWA administration and enforcement by the primacy agencies.

The America's Water Infrastructure Act of 2018 was the most comprehensive revision to SDWA since 1996. AWIA, contained a wide range of provisions designed to enhance drinking water quality, increase infrastructure investments, and bolster public health and safety. For example, section 2013 of AWIA requires community water systems that serve more than 3,300 people to develop or update risk and resilience assessments and emergency response plans.[1] These assessments and plans must address various components, including the resilience of physical and cyber infrastructure, monitoring practices, and strategies for responding to malevolent acts or natural hazards. Section 2013 also requires each water system to certify to the EPA that the system completed its risk and resilience assessment and emergency response plan, and established deadlines for these certifications.

Unlike other SDWA requirements, AWIA did not authorize the EPA to delegate implementation of assessment requirements to states, territories, and tribes. The EPA directly oversees elements of section 2013 of AWIA. Accordingly, the EPA issued guidance directly to water systems on the requirements, developed a certification system, and tracked compliance. Each EPA region worked with the water systems within its borders and had discretion over providing assistance and enforcement. Furthermore, section 2013 requires the EPA to provide, by August 2019, what the statute calls "baseline information on malevolent acts" relevant to water systems. The EPA issued this baseline information in August 2019 and updated it most recently in May 2024.

On February 12, 2013, the president issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, to further "the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats." The directive identified 16 critical infrastructure sectors and assigned roles and responsibilities for each sector to a federal agency, designating the EPA as the sector-specific agency responsible for the water and wastewater systems sector. According to the directive, the EPA was to provide, support, or facilitate technical assistance and consultations for water systems to identify vulnerabilities and help mitigate incidents. The directive also stated that "[c]ritical infrastructure must be secure and able to withstand and rapidly recover from all hazards," including:

> [A] threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

Under Presidential Policy Directive 21, the EPA is the sector specific agency responsible for ensuring that the nation's water sector is resilient to all threats and hazards by, among other things, "provid[ing] analysis, expertise, and other technical assistance to critical infrastructure owners and operators and

[1] 42 U.S.C. § 300i-2.

facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure."

On April 30, 2024, the White House issued National Security Memorandum 22, *National Security Memorandum on Critical Infrastructure Security and Resilience*. One of the reasons given for the memorandum's issuance was that the "United States is in the midst of a generational investment in the Nation's infrastructure"—a reference, in part, to the approximately $50 billion that the Infrastructure Investment and Jobs Act provided the EPA with to support the water and wastewater critical infrastructure sector. The memorandum further clarified federal roles and responsibilities for protecting critical infrastructure, directing CISA to coordinate with the Sector Risk Management Agencies to:

> [p]rovide technical and operational assistance, best practices based on existing standards and guidance to the greatest extent possible, and capacity development to State, local, Tribal, and territorial governments; other Federal entities; owners and operators; and international partners to enhance the security and resilience of critical infrastructure.

Similar to Presidential Policy Directive 21, National Security Memorandum 22 designated the EPA as the sector risk management agency for the water and wastewater systems sector.

In 2024, the OIG identified overseeing, protecting, and investing in water and wastewater systems sector as a top management challenge facing the EPA. The EPA has oversight responsibility for strengthening and securing the cyber and physical infrastructure at tens of thousands of public drinking water systems and publicly owned wastewater treatment systems. This critical infrastructure sector faces various threats from cyberattack, theft, vandalism, and other risks that can affect public health and leave communities vulnerable to the loss of clean water. This challenge is not hypothetical. Recent high-profile incidents at water systems have demonstrated the urgency needed to address cybersecurity weaknesses and vulnerabilities to physical attacks.

The OIG prioritized investigations into criminal and civil allegations of fraud or public corruption related to water systems that received funding from EPA programs. Through the Clean Water and Drinking Water State Revolving Funds, the EPA has partnered with the states to fund over $200 billion in water improvement projects through revolving low-cost loans and other financing options since the inception of these programs. And through the Water Infrastructure Finance and Innovation Act, the EPA has provided approximately $20 billion in long-term, low-cost supplemental loans for regionally and nationally significant projects and to state infrastructure financing authorities. The approximately $50 billion in Infrastructure Investment and Jobs Act funds to support the water and wastewater critical infrastructure sector from 2022 through 2026 is for the state revolving funds to, among other things, address aging water infrastructure and emerging contaminants. Additionally, the American Rescue Plan Act provided nearly $6.5 billion for water infrastructure projects. Our investigations, therefore, focus on

ensuring the integrity of those who are stewards of significant federal investment, including the integrity of the program and its recipients, subrecipients, and contractor.

Further, the OIG conducts oversight of the EPA's support of the water and wastewater critical infrastructure sector. For example, on November 21, 2022, the OIG issued Report No. 23-P-0003, *The EPA Met 2018 Water Security Requirements but Needs to Improve Oversight to Support Water System Compliance*, which assessed the adequacy of the cybersecurity baseline information that the EPA developed to meet the requirements of section 2013 of AWIA. We found, among other things, that the EPA had not provided adequate oversight to ensure community drinking water systems' compliance with AWIA requirements, including by not maintaining accurate contact information for water systems, by not publishing guidance regarding enforcement, by not providing sufficient assistance to support small water system compliance, or by not reviewing the quality of the Risk and Resilience Assessments and Emergency Response Plans. We concluded that community drinking water systems might therefore fail to meet AWIA requirements and may not understand their vulnerability to malevolent acts.

Recent EPA reports have found further issues with water system cybersecurity. For example, on May 20, 2024, the EPA issued an "enforcement alert," which outlined "the urgent cybersecurity threats and vulnerabilities to community drinking water systems and the steps these systems need to take to comply with the Safe Drinking Water Act." According to the EPA, its "inspectors have identified alarming cybersecurity vulnerabilities at drinking water systems across the country and taken actions to address them." The EPA concluded that over 70 percent of inspected water systems fail to comply with section 2013 of AWIA. The enforcement alert found that water systems had inadequate risk and resilience assessments and emergency response plans. In addition, the enforcement alert found significant failures in best practices, such as failure to change default passwords, use of single logins for all staff, and failure to curtail access by former employees.

The EPA has, since our November 2022 report, increased its outreach to water systems through, among other things, closer partnerships. The EPA administrator and the assistant to the president for National Security Affairs sent a letter to the state governors on March 18, 2024, requesting a "partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks." The letter described two recent threats to the water and wastewater critical infrastructure sector, noting that "[d]rinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices." The letter also highlighted resources from the EPA, other federal agencies, and private sector associations, including a link to guidance and resources to help water systems improve their cybersecurity posture, such as best practices, training materials, and technical assistance.

Concerns Identified: As part of our continued oversight of the EPA's role as a sector risk management agency, passive assessment of cybersecurity vulnerabilities was conducted on drinking water systems

with populations served of 50,000 people or greater. This consisted of a multilayered, passive assessment tool to scan the public-facing networks of 1,062 drinking water systems across the United States. The results identified cybersecurity vulnerabilities that an attacker could exploit to degrade functionality, cause loss or denial of service, or facilitate the theft of customer or proprietary information.

Cybersecurity Vulnerabilities at Drinking Water Systems

The passive assessment covered 1,062 drinking water systems for cybersecurity vulnerabilities that serve over 193 million people across the United States. Scan results for October 8, 2024, identified 97 drinking water systems serving approximately 26.6 million users as having either critical or high-risk cybersecurity vulnerabilities.

A non-linear scoring algorithm was used to prioritize the highest risk findings that should be addressed first. The findings are ranked by the 'score' and considers the impact of problem identified, risk to the organization, and number of times the problem has been observed.

The score impact of a finding is used to determine its risk level and can be in one of four levels grouped across the five categories; email security; IT Hygiene; Vulnerabilities; adversarial threats, and malicious activity:

- Critical – The finding has a score impact of > 7 points.
- High – The finding has a score impact between 4 and 7 points.
- Medium – The finding has a score impact between 2 and 4 points.
- Low – The finding has a score impact < 2 points.

Although not rising to a level of critical or high-risk cybersecurity vulnerabilities, an additional 211 drinking water systems, servicing over 82.7 million people, were identified as medium and low by having externally visible open portals.

Cybersecurity risks exist for all the facilities within drinking water systems. The methodology used for determining cybersecurity risks included mapping the digital footprint for each of the 1,062 drinking water systems. Drinking water systems can be comprised of many components, or facilities, that are located throughout a geographic area. Those facilities can include buildings and infrastructure used for the collection, pumping, treatment, storage, or distribution of drinking water. Over 75,000 IPs and 14,400 domains were analyzed for potential cyber vulnerabilities.

If malicious actors exploited the cybersecurity vulnerabilities we identified in our passive assessment, they could disrupt service or cause irreparable physical damage to drinking water infrastructure. According to a 2023 report from the US Water Alliance, a one-day disruption in water service across the United States could jeopardize $43.5 billion in economic activity. The following examples demonstrate

the potential impact of a cybersecurity-related water service disruption at two drinking water systems that have facilities that are comparable, in size and population served to many of the drinking water systems that we assessed.

Charlotte Water	California State Water Project
Charlotte Water serves over 890,000 people across six counties near Charlotte, North Carolina, and has an economic output of $48.5 billion from water-dependent industries.[2] We estimate that a water service disruption across all Charlotte Water facilities could potentially cost at least $132 million in lost revenue per day. Depending on the extent and location of damages, replacement costs for all facilities could exceed $5 billion.[3]	The California State Water Project serves over 27 million individuals, or more than two-thirds of California's population, and "supports an economy with a gross domestic product surpassing $2.25 trillion."[4] We estimate that a state-wide water service disruption could potentially cost at least $61 billion in lost revenue per day.

Issues with Reporting Cybersecurity Incidents to the EPA

While attempting to notify the EPA about the cybersecurity vulnerabilities, we found that the EPA does not have its own cybersecurity incident reporting system that water and wastewater systems could use to notify the EPA of cybersecurity incidents. Currently, the EPA relies on the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to provide this type of reporting information. Moreover, we were unable to find documented policies and procedures related to the EPA's coordination with the Cybersecurity and Infrastructure Security Agency and other federal and state authorities involved in sector-specific emergency response, security plans, metrics, and mitigation strategies. In August 2024, the Government Accountability Office released a report recommending that the EPA assess water and wastewater sector risk; develop and implement a national cybersecurity strategy; evaluate the sufficiency of its legal authorities to carry out its cybersecurity responsibilities; and seek additional authority as necessary.

My office is notifying you of these concerns so that the Agency may take whatever steps it deems appropriate. If you decide it is appropriate for your office to take or plan to take action to address these matters, the OIG would appreciate notification of that action. Should you have any questions regarding this report, please contact me at [redacted] or evans.nicolas@epa.gov.

cc: Sean W. O'Donnell, Inspector General
Ted Stanich, Associate Administrator, Office of National Security

[2] Charlotte Water, Economic Impact of Charlotte Water on the Regional Economy (2023).
[3] Charlotte Water, 2023 Annual Report: A Year of Flowing Progress (2023).
[4] State of California Department of Water Resources, The Economy of the State Water Project: Clean, Reliable, and Affordable Water for California (2023).

Whistleblower Protection

U.S. Environmental Protection Agency

The whistleblower protection coordinator's role is to educate Agency employees about prohibitions against retaliation for protected disclosures and the rights and remedies against retaliation. For more information, please visit the OIG's whistleblower protection webpage.

Contact us:

Congressional Inquiries: OIG.CongressionalAffairs@epa.gov

Media Inquiries: OIG.PublicAffairs@epa.gov

EPA OIG Hotline: OIG.Hotline@epa.gov

Web: epaoig.gov

Follow us:

X (formerly Twitter): @epaoig

LinkedIn: linkedin.com/company/epa-oig

YouTube: youtube.com/epaoig

Instagram: @epa.ig.on.ig

www.epaoig.gov