

**U.S. House Committee on Energy and Commerce**  
**Subcommittee on Environment, Manufacturing, and Critical Materials**  
**“Protecting Clean American Energy Production and Jobs by Stopping EPA’s**  
**Overreach”**  
**[January 31, 2024]**

1. Letter to Chairs Rodgers and Carter and Ranking Members Pallone and Tonko from Representative Christopher R. Deluzio, January 30, 2024, submitted by Rep. Pallone.
2. Letter to Chair Carter and Ranking Member Tonko from the Rural Community Assistance Partnership, January 31, 2024, submitted by the Majority.
3. DarkReading article entitled “Volt Typhoon Ramps Up Malicious Activity Against Critical Infrastructure,” January 11, 2024, submitted by the Majority.
4. A statement from Representative Anna G. Eshoo, January 31, 2024, submitted by the Minority.
5. A report from the Water Sector Coordinating Council entitled, “Cybersecurity 2021 State of the Sector” submitted by Rep. Clarke.
6. Letter to the Subcommittee on Environment, Manufacturing, and Critical Materials from the National Association of Clean Water Agencies and the Water Environment Federation, January 31, 2024, submitted by the Minority.
7. U.S. Department of Homeland Security Office of Inspector General report entitled “CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector” January 9, 2024, submitted by the Majority.

Congress of the United States  
House of Representatives  
Washington, DC 20515-3817

January 30, 2024

The Honorable Cathy McMorris Rogers  
Chair  
Energy and Commerce Committee  
United States House of Representatives  
Washington, D.C. 20515

The Honorable Frank Pallone  
Ranking Member  
Energy and Commerce Committee  
United States House of Representatives  
Washington, D.C. 20515

The Honorable Buddy Carter  
Chair  
Environment, Manufacturing,  
and Critical Materials Subcommittee  
Energy and Commerce Committee  
United States House of Representatives  
Washington, D.C. 20515

The Honorable Paul Tonko  
Ranking Member  
Environment, Manufacturing,  
and Critical Materials Subcommittee  
Energy and Commerce Committee  
United States House of Representatives  
Washington, D.C. 20515

Dear Chair McMorris Rogers, Ranking Member Pallone, Chair Carter, and Ranking Member Tonko:

Thank you for holding a hearing to examine cybersecurity threats to and the resilience of America's drinking water systems. I appreciate the committee's interest in this important issue, which is especially relevant to my constituents in Western Pennsylvania who recently experienced a cyberattack firsthand.

On November 25, 2023, an Iranian-backed cyber group, the "Cyber Av3ngers," attacked the Municipal Water Authority of Aliquippa by hacking Israeli-made equipment in the water system. The authority serves the City of Aliquippa and Raccoon, Potter, and portions of Hopewell Townships in Beaver County. Thankfully, the attack did not interrupt my constituents' water service or compromise their personal information, but such risks are obvious. Any attack on our nation's critical infrastructure is of significant concern, and Congress must work in a bipartisan way to ensure water systems and others have the necessary protections.

To that end, Congress should give the Environmental Protection Agency (the Sector Risk Management Agency) the tools and resources it needs to support and coordinate with the water sector to prepare for and build resilience against risks like cyber threats. I look forward to

working with the Energy and Commerce Committee, as the committee of jurisdiction, to address this important issue and give our fellow Americans the peace of mind they ought to have that water systems and other critical infrastructure are secured.

Very respectfully,

A handwritten signature in blue ink that reads "Christopher R. Deluzio". The signature is written in a cursive style with a prominent initial "C".

Chris Deluzio  
Member of Congress



January 31, 2024

Representative Buddy Carter  
Chair, House Subcommittee on Environment,  
Manufacturing, and Critical Materials  
2432 Rayburn House Office Building  
Washington, DC, 20515

Representative Paul Tonko  
Ranking Member, House Subcommittee on  
Environment, Manufacturing, and Critical Materials  
2463 Rayburn House Office Building  
Washington, DC 20515

Dear Chair Carter and Ranking Member Tonko,

On behalf of the Rural Community Assistance Partnership (RCAP) – a national network of non-profit partners working to provide technical assistance, training, and resources to rural and Tribal communities in every state and territory, and on Tribal lands and Colonias – I write to thank you for your continued support for rural water and for holding today’s hearing on ensuring the cybersecurity of drinking water systems.

Water systems in small, rural, and underserved communities face unique challenges when it comes to building the capacity to carry out necessary capital infrastructure upgrades and to manage day-to-day operations and maintenance activities. Rural systems are often run by volunteers or one or two full-time staff members, and because of these systems’ relatively small number of ratepayers, they struggle disproportionately to develop the economies of scale needed to have cash on hand for new or unexpected costs. Many times, our assistance and the availability of federal resources provide the only pathway to getting necessary work done to ensure the continued reliability of utility services for their community.

The emerging prevalence of water system cybersecurity concerns in the past few years – and particularly in recent months with the new wave of attacks from foreign actors with ties to Iran – now adds to the list of complex and costly factors utility managers must address to ensure the safety and reliability of their systems. This is particularly concerning for many of the small, rural systems we work with, as limited financial and staff resources make it far more difficult for them to develop the capacity needed to implement robust cyber protections.

To take on this immense challenge, small, rural systems need better educational resources regarding their vulnerability and the urgent need to address it, and, critically, need for there to be increased, flexible federal funding and technical assistance resources made available for this purpose. For the well over 100,000 small systems serving communities of 3,300 or less across the U.S., awareness of their susceptibility and best practices to address it alone are not enough to solve this issue, as many are juggling a handful of immediate responsibilities with already stretched-thin financial and staff resources.

Congress must address this by providing robust funding and technical assistance provisions to help small systems broadly take up durable cybersecurity protection practices and to assist communities with adding cybersecurity to their required Risk and Resilience Assessments under the Safe Drinking Water Act. RCAP and its network stand ready to help the federal government implement these resources in rural communities across the U.S.

The provision of safe and clean water is essential to the health and sustainability of all communities, and protection from cybersecurity concerns is an important part of this mission. We look forward to working with you and your colleagues to ensure small, rural communities have the federal funding and technical assistance resources they need to address this emerging threat.

Thank you,

DocuSigned by:  
*Olga Morales Pate*  
Olga Morales-Pate

CEO, Rural Community Assistance Partnership

CYBER RISK

THREAT INTELLIGENCE

VULNERABILITIES & THREATS

# Volt Typhoon Ramps Up Malicious Activity Against Critical Infrastructure

The Chinese state-sponsored APT has compromised as many as 30% of Cisco legacy routers on a SOHO botnet that multiple threat groups use.



Jai Vijayan, Contributing Writer  
January 11, 2024

4 Min Read



China-backed cyber espionage group Volt Typhoon is systematically targeting legacy Cisco devices in a sophisticated and stealthy campaign to grow its attack infrastructure.

In many instances, the threat actor, known for targeting critical infrastructure, is exploiting a couple of vulnerabilities from 2019 in routers, to break into target devices and take control of them.

## Targeting US Critical Infrastructure Sectors

Researchers from SecurityScorecard's threat intelligence team spotted the activity when doing some follow-up investigations on recent vendor and [media reports](#) about Volt Typhoon breaking into US critical infrastructure organizations and laying the ground for potential future disruptions. The attacks have targeted water utilities, power suppliers, transportation, and communications systems. The group's victims have included organizations in the US, UK, and Australia.

One of the vendor reports, from [Lumen](#), described a botnet comprised of [small office/home office \(SOHO\) routers](#) that Volt Typhoon — and other Chinese threat groups — is using as a command-and-control (C2) network in attacks against high-value networks. The network that Lumen described in the report consists mainly of end-of-life routers from Cisco, DrayTek, and, to a smaller extent, Netgear.

SecurityScorecard researchers used the indicators of compromise (IoCs) that Lumen released with its report to see if they could identify new infrastructure associated with Volt Typhoon's campaign. The [investigation](#) showed the threat group's activity may be more extensive than previously thought, says Rob Ames, staff threat researcher at SecurityScorecard.

For example, Volt Typhoon appears to have been responsible for compromising as much as 30% — or 325 of 1,116 — of end-of-life Cisco RV320/325 routers that SecurityScorecard

observed on the C2 botnet over a 37-day period. The security vendor's researchers observed regular connections between the compromised Cisco devices and known Volt Typhoon infrastructure between Dec. 1, 2023 and Jan. 7, 2024, suggesting a very active operation.

SecurityScorecard's digging also showed Volt Typhoon deploying "fy.sh", a hitherto unknown Web shell on the Cisco routers and other network edge devices that the group is currently targeting. In addition, SecurityScorecard was able to identify multiple new IP addresses that appeared linked to Volt Typhoon activity.

"SecurityScorecard used previously circulated IoCs linked to Volt Typhoon to identify the newly compromised devices we observed, the previously unspecified webshell (fy.sh), and the other IP addresses that may represent new IoCs," Ames says.

## Living-off-the-Land Cyberattacks

[Volt Typhoon](#) is a threat group that the [US Cybersecurity and Infrastructure Agency \(CISA\)](#) has identified as a state-sponsored Chinese threat actor targeting US critical infrastructure sectors. [Microsoft](#), the first to report on the group back in May 2023, has described it as being active since at least May 2021, being based in China, and conducting large-scale cyber espionage using a slew of living-off-the-land techniques. The company has assessed the group as developing capabilities to disrupt critical communications capabilities between the US and Asia during potential future conflicts.

Ames says Volt Typhoon's use of compromised routers for data transfers is one indication of the group's commitment to stealth.

"The group often routes its traffic through these devices in order to avoid geographically based detection when targeting organizations in the same area as the compromised routers," he says. "These organizations may be less likely to notice malicious activity if the traffic involved appears to originate from the area in which the organization is based."

## Cyber-Targeting of Vulnerable End-of-Life Gear

Volt Typhoon's targeting of end-of-life devices also makes a lot of sense from the attacker's perspective, Ames says. There are some 35 known critical vulnerabilities with a severity rating of at least 9 out of 10 on the CVSS scale — including two in CISA's Known Exploited Vulnerabilities catalog — associated with the Cisco RV320 routers that Volt Typhoon has been targeting. Cisco stopped issuing any bug fixes, maintenance releases, and repairs for



the technology three years ago, in January 2021. In addition to the Cisco devices, the Volt Typhoon-linked botnet also includes compromised legacy DrayTek Vigor and Netgear ProSafe routers.

"From the perspective of the devices themselves, they're low-hanging fruit," Ames says. "Since 'end-of-life' means that the devices' producers will no longer issue updates for them, vulnerabilities affecting them are likely to go unaddressed, leaving the devices susceptible to compromise."

Callie Guenther, senior manager of cyber threat research at Critical Start, says Volt Typhoon's strategic targeting of end-of-life Cisco routers, its development of custom tools like fy.sh, and its geographical and sectoral targeting suggest a highly sophisticated operation.

"Focusing on legacy systems is not a common tactic among threat actors, primarily because it requires specific knowledge about older systems and their vulnerabilities, which might not be widely known or documented," Guenther says. "However, it is a growing trend, especially among state-sponsored actors who have the resources and motivation to conduct extensive reconnaissance and develop tailored exploits."

As examples, she points to multiple threat actors targeting the so-called [Ripple20 vulnerabilities](#) in a TCP/IP stack that affected millions of legacy IoT devices, as well as Chinese and Iranian threat groups targeting flaws in older VPN products.

## About the Author(s)



**Jai Vijayan, Contributing Writer**

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year career at...

Keep up with the latest cybersecurity threats, newly discovered vulnerabilities, data breach information, and emerging trends.  
Delivered daily or weekly right to your email inbox.

SUBSCRIBE

## You May Also Like

---

**Cyber Risk** Why Generative AI Will Be a Major Driver of Cybersecurity Threats

**Cyber Risk** How AI is Shaping Cyber Future With US Treasury Partnership, Collaborations

**Cyber Risk** How AI is Shaping Oman's Economic Backbone

**Cyber Risk** Why AI is a Better Way to Manage Cloud Risk

## More Insights

---

### Webinars

**Tips for Managing Cloud Security in a Hybrid Environment**

FEB 01, 2024

**Top Cloud Security Threats Targeting Enterprises**

FEB 08, 2024

## DevSecOps: The Smart Way to Shift Left

FEB 14, 2024

## Making Sense of Security Operations Data

FEB 21, 2024

## Your Everywhere Security Guide: 4 Steps to Stop Cyberattacks

FEB 27, 2024

---

### More Webinars

### Events

Cybersecurity's Hottest New Technologies - Dark Reading March 21 Event

Black Hat Asia - April 16-19 - [Learn More](#)

Black Hat Spring Trainings - March 12-15 - [Learn More](#)

Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What

---

### More Events

## Editor's Choice

CYBERSECURITY OPERATIONS



CYBERATTACKS & DATA BREACHES



## Microsoft Shares New Guidance in Wake of 'Midnight Blizzard' Cyberattack

by Jai Vijayan, Contributing Writer

JAN 26, 2024

4 MIN READ

CYBER RISK

VULNERABILITIES & THREATS

## New Jersey School District Shut Down by Cyberattack

by Kristina Beek, Associate Editor, Dark Reading

JAN 29, 2024

1 MIN READ

### Reports

Passwords Are Passe: Next Gen Authentication Addresses Today's Threats

**The State of Supply Chain Threats**

**How to Deploy Zero Trust for Remote Workforce Security**

**What Ransomware Groups Look for in Enterprise Victims**

**The Rise of the No-Code Economy**

[More Reports](#)

## White Papers

**Threat Terrain of the Modern Factory: Survey of Programmable Assets and Robot Software**

**Pixelle's OT Security Triumph with Security Inspection**

**IT Zero Trust vs. OT Zero Trust: It's all about Availability**

**The OT Zero Trust Handbook: Implementing the 4 Cornerstones of OT Security**

**2023 Software Supply Chain Attack Report**

[More Whitepapers](#)

## Events

**Cybersecurity's Hottest New Technologies - Dark Reading March 21 Event**

MAR 21, 2024

**Black Hat Asia - April 16-19 - Learn More**

APR 16, 2024

**Black Hat Spring Trainings - March 12-15 - Learn More**

MAR 12, 2024

**Cyber Resiliency 2023: How to Keep IT Operations Running, No Matter What**

AUG 24, 2023

[More Events](#)

## **DARK**READING

### **Discover More With Informa Tech**

[Black Hat](#)

[Omdia](#)

### **Working With Us**

[About Us](#)

[Advertise](#)

[Reprints](#)

### **Join Us**

[NEWSLETTER SIGN-UP](#)

### **Follow Us**







**Statement for the Record of Rep. Anna Eshoo**

Ensuring the Cybersecurity of America's Drinking Water Systems  
*House Subcommittee on Environment, Manufacturing, and Critical Materials*  
January 31, 2024

Thank you, Chairman Carter and Ranking Member Tonko, for holding this important hearing, and my thanks to the witnesses for your expert testimony and your important work to provide safe and reliable water services to Americans.

The security of our nation's water utilities is of the utmost importance. As a cybersecurity champion in my 30 years in Congress, I've have grown increasingly concerned about the cyber risks facing public water systems.

Local governments and utility infrastructure are increasingly threatened by cyberattacks, such as the January 2021 attack when a hacker tried to poison a water treatment plant in Discovery Bay, California that serves parts of the San Francisco Bay Area, not far from my congressional district.

In fact, many of the over 52,000 water systems in the country are similarly vulnerable, operating without even the most basic cybersecurity protections. Many use default passwords or operate on unsecured internet networks, often because they lack the time, money, and expertise necessary to implement cybersecurity protections. This problem is not unique to water systems, and it's why I've previously introduced the *Improving Cybersecurity of Small Businesses, Nonprofits, and Local Governments Act* to address these kinds of issues by requiring CISA and the SBA to provide voluntary training and technical assistance to smaller organizations like water utilities that are vulnerable to cyberattacks.

Last year, the EPA took action and issued an interpretative memo requiring states to include basic cybersecurity questions as part of their regular sanitary surveys of water systems and to provide support in remedying any issues. The EPA rescinded the memo in the face of pending litigation, and is now instead making similar voluntary recommendations.

In November, our worst fears were confirmed when the EPA, FBI, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Israeli National Cyber Directorate warned that many of these water control facilities have since been compromised by Iranian hackers.

Basic cybersecurity protections are necessary for any organization in the 21<sup>st</sup> century, particularly those serving the public. Cyberattacks can lead to serious damage that ratepayers will be accountable for, or worse, threaten the health and safety of those who rely on America's many small water systems for safe, clean drinking water. It's imperative that water systems have both minimum standards and the resources to implement them to protect Americans from these threats.

# WATER AND WASTEWATER SYSTEMS

# CYBERSECURITY

## 2021 STATE OF THE SECTOR

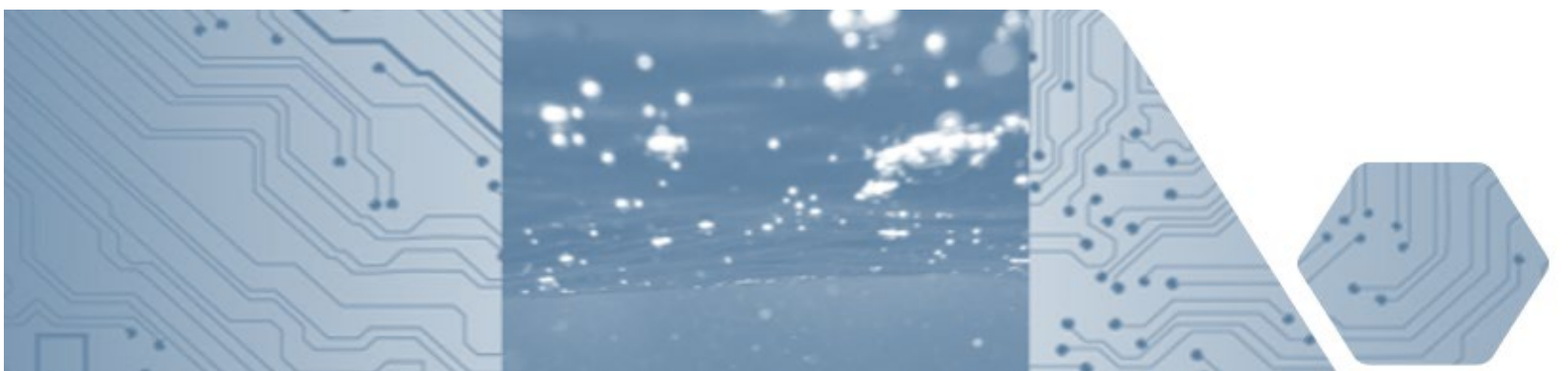


## Water Sector Coordinating Council



**JUNE 2021**

|  |    |
|--|----|
| Executive Summary.....                               | 2  |
| Cybersecurity Needs in the Sector .....              | 5  |
| Service and Ownership Structure .....                | 7  |
| Frequency of Risk Assessments .....                  | 9  |
| Risk Management Plans Addressing Cybersecurity ..... | 10 |
| Risk Management Challenges.....                      | 10 |
| Information-Sharing Concerns.....                    | 11 |
| Cybersecurity Program Challenges.....                | 12 |
| IT- and OT-networked Assets.....                     | 13 |
| IT and OT Management and Workforce .....             | 16 |
| Current Focus on Cybersecurity as a Priority.....    | 18 |
| Cybersecurity Resources Used in the Sector.....      | 18 |
| Training .....                                       | 19 |
| Next Steps.....                                      | 21 |



## Executive Summary

With threats from increasingly sophisticated and destructive attackers, cybersecurity has become a top priority for water and wastewater systems. Recent incidents have added urgency to discussions within the sector and with Congress and in federal agencies on how best to help utilities improve their cybersecurity.

To help guide discussions with policymakers and to inform the sector's own cybersecurity programs, the Water Sector Coordinating Council (WSCC) - an advisory body comprising the national water and wastewater associations, the sector's research foundation and WaterISAC - collaborated on a utility survey to develop a picture of current cybersecurity practices in the sector to better articulate the challenges and needs of the sector.

This voluntary survey was distributed to utilities across the country by the nation's water and wastewater associations. The results represent a first-of-its-kind snapshot of the Water and Wastewater Systems Sector cybersecurity posture.

The survey, conducted in April 2021, resulted in 606 responses from water and wastewater utilities. The results show a range of cybersecurity preparedness levels across the sector, with many excelling in their efforts with current resources but with others demonstrating room for improvement and a need for greater support.

# Water Sector Coordinating Council

## Member Organizations

- American Water Works Association
- Association of Metropolitan Water Agencies
- National Association of Water Companies
- National Association of Clean Water Agencies
- National Rural Water Association
- Water Environment Federation
- Water Information Sharing and Analysis Center
- The Water Research Foundation

The Water Sector Coordinating Council is a policy, strategy and coordination mechanism for the sector in interactions with the government and other sectors on critical infrastructure security and resilience issues.

## Challenges

Like all sectors, water and wastewater systems are targets, directly or indirectly, of cyber attackers, but complicating any set of solutions is the demographics of the sector. There are approximately 52,000 community water systems and approximately 16,000 wastewater systems in the United States.

Among these utilities are a wide range of capabilities and capacities for cybersecurity enhancement. Many are subject to economic disadvantages typical of rural and urban communities. Others do not have access to a cybersecurity workforce. Operating in the background is that these utilities are struggling to maintain and replace infrastructure, maintain revenues while addressing issues of affordability, and comply with safe and clean water regulations.

## Needs

Survey respondents identified several needs to help them improve cybersecurity.

The top four categories are:

- Training and education specific to the water sector,
- Technical assistance, assessments, and tools,
- Cybersecurity threat information, and
- Federal loans and grants.

With the exception of federal loans and grants, many such resources already exist between those developed by the sector itself and those contributed by federal agencies. But clearly there is a need for additional resources in order to reach a greater audience among our large and diverse sector. The development and promotion of these resources will require a combined effort between the sector, government agencies, and partners.

Further, nearly 30% indicated a need for information technology (IT) and operational technology (OT) supply chain integrity, which demands strong federal leadership.

### Respondents by Job Type

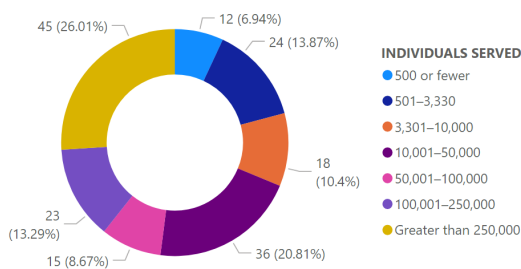
| ANSWER CHOICES                                   | RESPONSES |     |
|--|-----------|-----|
| CIO, CTO, CFO                                    | 9.76%     | 48  |
| CISO, Sr. Security Analyst, System Administrator | 7.93%     | 39  |
| IT Manager, IT Specialist                        | 14.84%    | 73  |
| Other Executive Management or Board Member       | 28.46%    | 140 |
| Water Engineer, Operations Director              | 39.02%    | 192 |
| TOTAL  |           | 492 |

# Cybersecurity Needs in the Sector

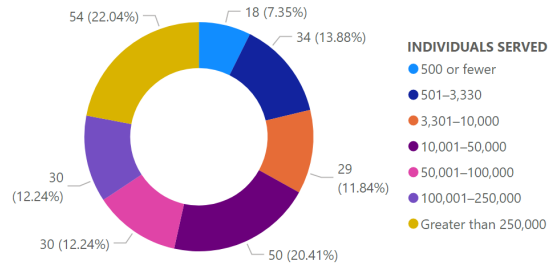
The following sector needs were identified by respondents. Further breakdown of needs by utility size are provided in the charts below.

| ANSWER CHOICES  | RESPONSES  |
|---|------------|
| Technical assistance, advice, assessments or other support              | 47.47% 282 |
| Federal grants or loans for cybersecurity equipment or services         | 41.08% 244 |
| Training and education targeting the water sector                       | 51.01% 303 |
| Assurance of supply chain integrity for IT and OT hardware and software | 29.12% 173 |
| Funding to hire cybersecurity personnel                                 | 29.80% 177 |
| Cybersecurity threat information  | 41.25% 245 |
| I'm not sure  | 17.68% 105 |
| No assistance is needed   | 12.46% 74  |
| <b>Total Respondents: 594</b>   |            |

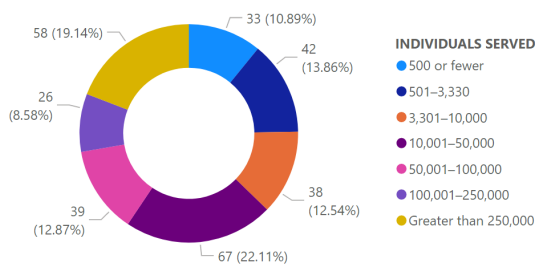
Count of NEED Assurance of supply chain integrity for IT and OT hardware and software by INDIVIDUALS SERVED



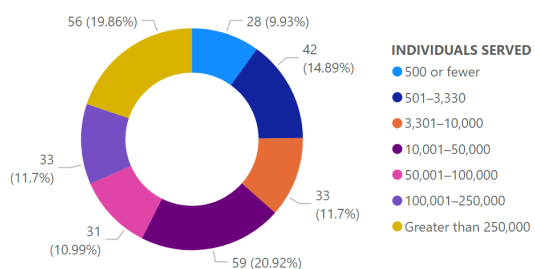
Count of NEED Cybersecurity threat information by INDIVIDUALS SERVED



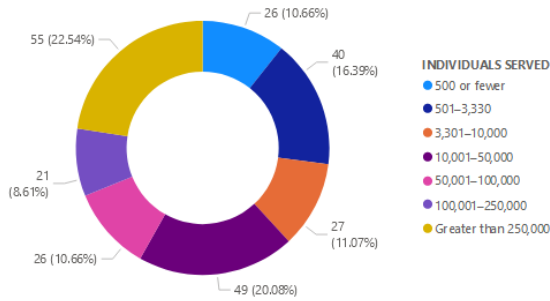
Count of NEED Training and education targeting the water sector by INDIVIDUALS SERVED



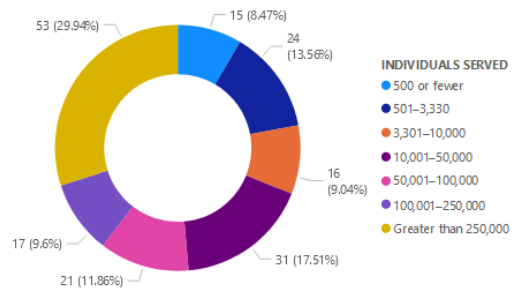
Count of NEED Technical assistance, advice, assessments or other support by INDIVIDUALS SERVED



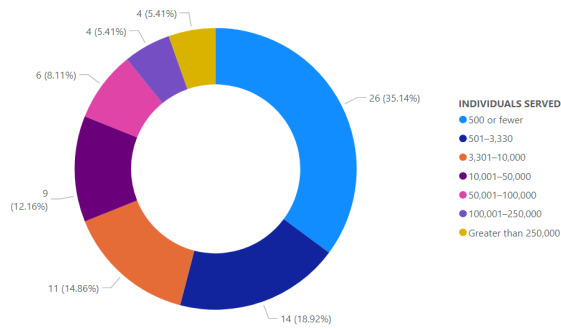
Count of NEED Federal grants or loans for cybersecurity equipment or services by INDIVIDUALS SERVED



Count of NEED Funding to hire cybersecurity personnel by INDIVIDUALS SERVED



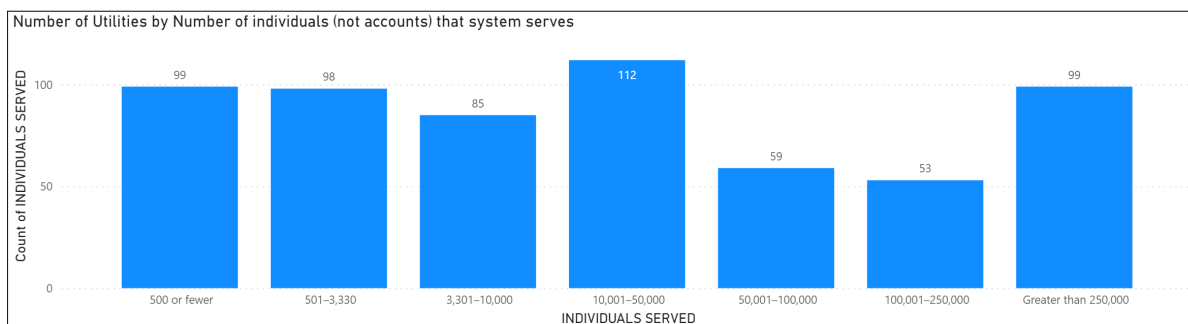
Count of NEED No assistance is needed by INDIVIDUALS SERVED





## Service and Ownership Structure

| PRIMARY SERVICE AND OWNERSHIP STRUCTURE |  |                                |                                   |   |            |
|---|--|--------------------------------|-----------------------------------|---|------------|
| PRIMARY SERVICE                         | Department of a municipality or county | Private non-profit/cooperative | Privately owned or investor-owned | Special district or independent government entity | Total      |
| Combined Drinking Water and Wastewater  | 196                                    | 12                             | 15                                | 77  | 300        |
| Drinking Water Only                     | 90                                     | 43                             | 22                                | 87  | 242        |
| Wastewater Only                         | 25                                     | 1                              | 2                                 | 34  | 62         |
| <b>Total</b>                            | <b>311</b>                             | <b>56</b>                      | <b>39</b>                         | <b>198</b>  | <b>604</b> |



**51.4%** of survey respondents are with a department of a **municipality** or county.

**32.7%** of survey respondents are with a **special district** or independent government entity.

**9.3%** of survey respondents are with a **private non-profit/cooperative**. **6.4%** of survey respondents are with a **privately-owned or investor-owned utility**.

**49.8%** of survey respondents represent **combined drinking water and wastewater systems**. **40%** of survey respondents represent **drinking water-only systems**. And **10.2%** of respondents represent **wastewater-only systems**.

| PERCENT UTILITY 2021 BUDGET ALLOCATION FOR IT CYBERSECURITY                             | 500 or fewer | 501–3,330 | 3,301–10,000 | 10,001–50,000 | 50,001–100,000 | 100,001–250,000 | Greater than 250,000 | Total      |
|---|--------------|-----------|--------------|---------------|----------------|-----------------|----------------------|------------|
| 1%–5%   | 6            | 19        | 18           | 26            | 20             | 12              | 29                   | <b>130</b> |
| 6%–10%  | 1            |           | 4            | 10            | 4              | 6               | 12                   | <b>37</b>  |
| Don't know  | 17           | 15        | 20           | 23            | 14             | 17              | 28                   | <b>134</b> |
| Greater than 10%  | 1            | 3         | 4            | 4             |                | 3               | 9                    | <b>24</b>  |
| Less than 1%  | 64           | 54        | 33           | 33            | 13             | 11              | 14                   | <b>222</b> |
| Not applicable; IT cybersecurity is managed at the municipal or county government level | 6            | 3         | 5            | 11            | 7              | 3               | 4                    | <b>39</b>  |
| <b>Total</b>  | <b>95</b>    | <b>94</b> | <b>84</b>    | <b>107</b>    | <b>58</b>      | <b>52</b>       | <b>96</b>            | <b>586</b> |

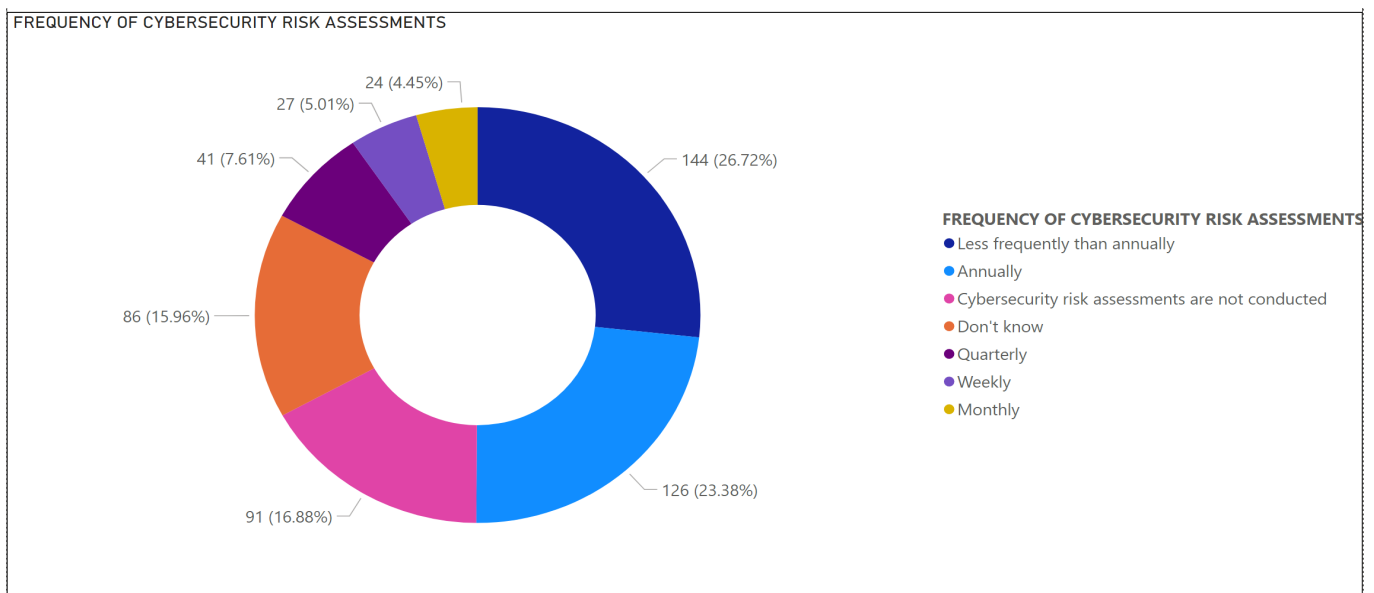
| PERCENT UTILITY 2021 BUDGET ALLOCATION FOR OT CYBERSECURITY                             | 500 or fewer | 501–3,330 | 3,301–10,000 | 10,001–50,000 | 50,001–100,000 | 100,001–250,000 | Greater than 250,000 | Total      |
|---|--------------|-----------|--------------|---------------|----------------|-----------------|----------------------|------------|
| 1%–5%   | 8            | 19        | 14           | 26            | 15             | 15              | 26                   | <b>123</b> |
| 6%–10%  |              |           | 3            | 10            | 2              | 5               | 9                    | <b>29</b>  |
| Don't know  | 19           | 17        | 21           | 25            | 12             | 13              | 30                   | <b>137</b> |
| Greater than 10%  | 1            | 1         | 3            |               |                | 2               | 3                    | <b>10</b>  |
| Less than 1%  | 62           | 54        | 40           | 39            | 26             | 14              | 28                   | <b>263</b> |
| Not applicable; OT cybersecurity is managed at the municipal or county government level | 5            | 3         | 3            | 8             | 3              | 3               |                      | <b>25</b>  |
| <b>Total</b>  | <b>95</b>    | <b>94</b> | <b>84</b>    | <b>108</b>    | <b>58</b>      | <b>52</b>       | <b>96</b>            | <b>587</b> |

A representative sampling across all size systems provides the following 2021 budget allocations for cybersecurity:

- 38% of systems allocate less than 1% of budget to **IT** cybersecurity.
- 22.1% of systems allocate 1–5% of budget to **IT** cybersecurity.
- 6.3% of systems allocate 6–10% of budget to **IT** cybersecurity.
- 4.1% of systems allocate greater than 10% of budget to **IT** cybersecurity.
- 44.8% of systems allocate less than 1% of budget to **OT** cybersecurity.
- 20.95% of systems allocate 1–5% of budget to **OT** cybersecurity.
- 4.9% of systems allocate 6–10% of budget to **OT** cybersecurity.
- 1.7% of systems allocate greater than 10% of budget to **OT** cybersecurity.

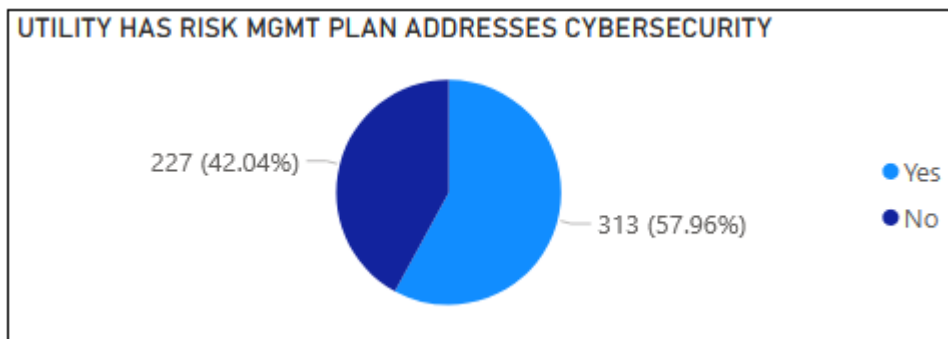
## Frequency of Risk Assessments

Risk assessment is defined as the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk management includes threat and vulnerability analyses as well as analyses of adverse effects on individuals arising from information processing and considers mitigations provided by security and privacy controls planned or in place. Synonymous with risk analysis. [NIST SP 800-53r5]



**23.38% of systems surveyed perform cybersecurity risk assessments annually.** 7.61% of systems are conducting quarterly cybersecurity risk assessments and 5% of systems are conducting weekly cybersecurity risk assessments.

## Risk Management Plans Addressing Cybersecurity



More than half of the systems surveyed (57.96%) have a risk management plan that addresses cybersecurity.

## Risk Management Challenges

Responses varied by system type regarding risk management challenges. The **top three challenges by primary service** include:

- **Combined drinking water and wastewater systems:** 1. minimizing control system exposure; 2. assessing risks; and 3. identifying and remediation hardware or software vulnerabilities.
- **Drinking water systems:** 1. assessing risks; 2. awareness of cybersecurity threats and best practices; and 3. planning for emergencies, incidents and disasters.
- **Wastewater systems:** 1. minimizing control system exposure; 2. securing remote access to the OT system; and 3. assessing risks.

The **number one challenge** for systems serving more than 100,000 is **creating a cybersecurity culture within the utility**.

**Awareness of threats and best practices** was the top challenge for systems serving between 3,300 and 50,000 people.


## Information-Sharing Concerns

The following high priority concerns were identified regarding the exchange of organizational information on cybersecurity threats, vulnerabilities, mitigation, and security incidents with external organizations:

| ANSWER CHOICES  | RESPONSES |     |
|---|-----------|-----|
| Lack of trust around my utility information being kept confidential | 22.39%    | 118 |
| Lack of credible information shared by other organizations          | 12.33%    | 65  |
| Lack of know-how (who to share information with or how to do so)    | 37.76%    | 199 |
| Lack of value, nothing gained in return                             | 11.57%    | 61  |
| None of the above (no barriers to information sharing with others)  | 30.36%    | 160 |
| Don't know  | 16.89%    | 89  |
| Total Respondents: 527  |           |     |

## Cybersecurity Program Challenges

Respondents gauged the extent that the following issues are a challenge for their organization's cybersecurity program. The purpose of this question was to capture elements of cybersecurity that are difficult to address.

|   | MINOR         |  |               |               | SIGNIFICANT  | TOTAL | WEIGHTED AVERAGE |
|---|---------------|---|---------------|---------------|--------------|-------|------------------|
| Website security                          | 34.78%<br>176 | 24.90%<br>126   | 21.74%<br>110 | 10.47%<br>53  | 8.10%<br>41  | 506   | 2.32             |
| Information sharing                       | 33.14%<br>168 | 21.89%<br>111   | 26.23%<br>133 | 11.83%<br>60  | 6.90%<br>35  | 507   | 2.37             |
| Cloud security                            | 28.46%<br>144 | 18.77%<br>95  | 26.09%<br>132 | 14.82%<br>75  | 11.86%<br>60 | 506   | 2.63             |
| Physical security                         | 24.11%<br>122 | 24.51%<br>124   | 26.68%<br>135 | 15.02%<br>76  | 9.68%<br>49  | 506   | 2.62             |
| Incident response                         | 19.08%<br>95  | 19.08%<br>95  | 25.90%<br>129 | 21.69%<br>108 | 14.26%<br>71 | 498   | 2.93             |
| Awareness training program                | 18.38%<br>93  | 21.94%<br>111   | 27.67%<br>140 | 19.57%<br>99  | 12.45%<br>63 | 506   | 2.86             |
| Device security                           | 15.98%<br>81  | 23.27%<br>118   | 29.98%<br>152 | 19.33%<br>98  | 11.44%<br>58 | 507   | 2.87             |
| Business continuity and disaster recovery | 15.67%<br>79  | 19.05%<br>96  | 25.60%<br>129 | 20.83%<br>105 | 18.85%<br>95 | 504   | 3.08             |
| Risk assessment and management            | 15.32%<br>78  | 18.07%<br>92  | 32.22%<br>164 | 20.04%<br>102 | 14.34%<br>73 | 509   | 3.00             |

## IT- and OT-networked Assets

Information technology, or IT, refers to the business or enterprise network of a utility. This includes computers, software, firmware and similar procedures and services, such as email, websites, bill payment and customer management systems, and work order applications.

Operational technology, or OT, refers to required programmable systems that manage devices, monitor and control physical processes and events of a utility. OT includes industrial control systems, such as supervisory control and data acquisition (SCADA) systems; fire control systems; and physical access control mechanisms.

Identifying IT and OT assets is a critical first step in improving cybersecurity. An organization cannot protect what it cannot see.

37.9% of utilities have identified all IT-networked assets, with an additional 21.7% working to identify all IT-networked assets.

| HAS UTILITY IDENTIFIED IT-NETWORKED ASSETS            | 500 or fewer | 501–3,330 | 3,301–10,000 | 10,001–50,000 | 50,001–100,000 | 100,001–250,000 | Greater than 250,000 | Total     |            |
|---|--------------|-----------|--------------|---------------|----------------|-----------------|----------------------|-----------|------------|
| All IT-networked assets have been identified          | 1            | 12        | 12           | 26            | 44             | 23              | 30                   | 56        | 204        |
| Don't know  |              | 28        | 24           | 24            | 21             | 10              | 8                    | 5         | 120        |
| No work has been done to identify IT-networked assets |              | 38        | 35           | 8             | 9              | 2               | 2                    | 3         | 97         |
| Work is underway to identify IT-networked assets      |              | 6         | 15           | 20            | 24             | 20              | 12                   | 20        | 117        |
| <b>Total</b>  | <b>1</b>     | <b>84</b> | <b>86</b>    | <b>78</b>     | <b>98</b>      | <b>55</b>       | <b>52</b>            | <b>84</b> | <b>538</b> |

30.5% of utilities have identified all OT-networked assets, with an additional 22.5% working to identify all OT-networked assets.

| HAS UTILITY IDENTIFIED OT-NETWORKED ASSETS            | 500 or fewer | 501–3,330 | 3,301–10,000 | 10,001–50,000 | 50,001–100,000 | 100,001–250,000 | Greater than 250,000 | Total     |            |
|---|--------------|-----------|--------------|---------------|----------------|-----------------|----------------------|-----------|------------|
| All OT-networked assets have been identified          | 1            | 8         | 9            | 21            | 35             | 19              | 31                   | 40        | 164        |
| Don't know  |              | 31        | 28           | 28            | 29             | 13              | 7                    | 13        | 149        |
| No work has been done to identify OT-networked assets |              | 40        | 37           | 9             | 9              | 3               | 4                    | 1         | 103        |
| Work is underway to identify OT-networked assets      |              | 5         | 12           | 19            | 25             | 20              | 10                   | 30        | 121        |
| <b>Total</b>  | <b>1</b>     | <b>84</b> | <b>86</b>    | <b>77</b>     | <b>98</b>      | <b>55</b>       | <b>52</b>            | <b>84</b> | <b>537</b> |

The following responses were provided in response to the question “For identified networked IT and OT assets, what is the status of your utility’s cyber protection efforts?”

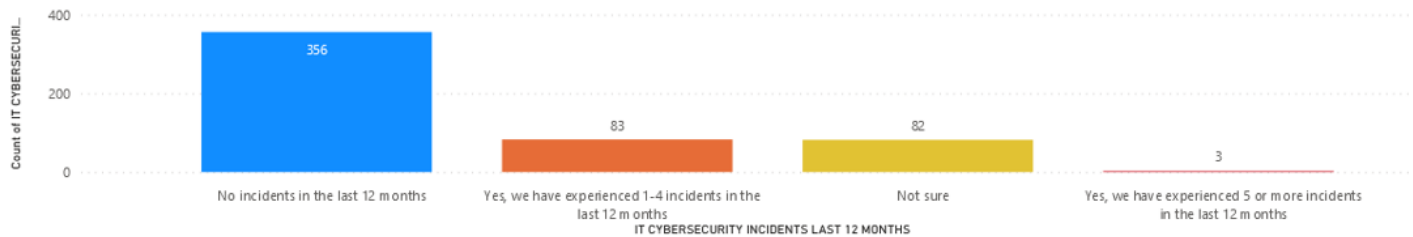
Nearly 75% of respondents report they have implemented efforts or are in some stage of progress.

| ANSWER CHOICES   | RESPONSES |            |
|--|-----------|------------|
| No progress/no current plans to conduct cyber protection efforts           | 25.47%    | 135        |
| Planning to conduct cyber protection efforts                               | 15.47%    | 82         |
| Cyber protection efforts are in progress                                   | 36.60%    | 194        |
| Cyber protection efforts have been implemented and are monitored regularly | 22.45%    | 119        |
| <b>TOTAL</b>   |           | <b>530</b> |

IT cybersecurity incident: A violation or imminent threat of violation to the confidentiality, integrity, or availability of IT systems and/or data.

OT cybersecurity incident: A violation or imminent threat of violation to the availability, integrity, or confidentiality of OT systems and/or data.

IT CYBERSECURITY INCIDENTS LAST 12 MONTHS



OT CYBERSECURITY INCIDENTS LAST 12 MONTHS



67.9% of systems reported no IT cybersecurity incidents in the last twelve months.

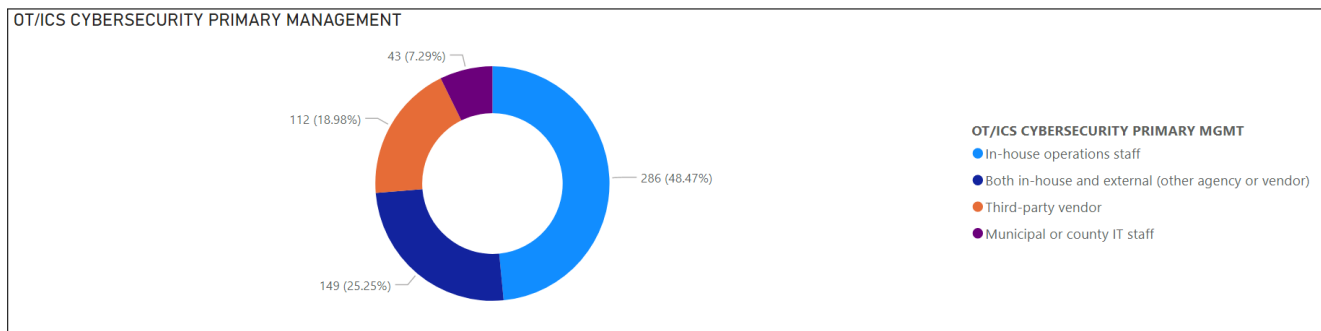
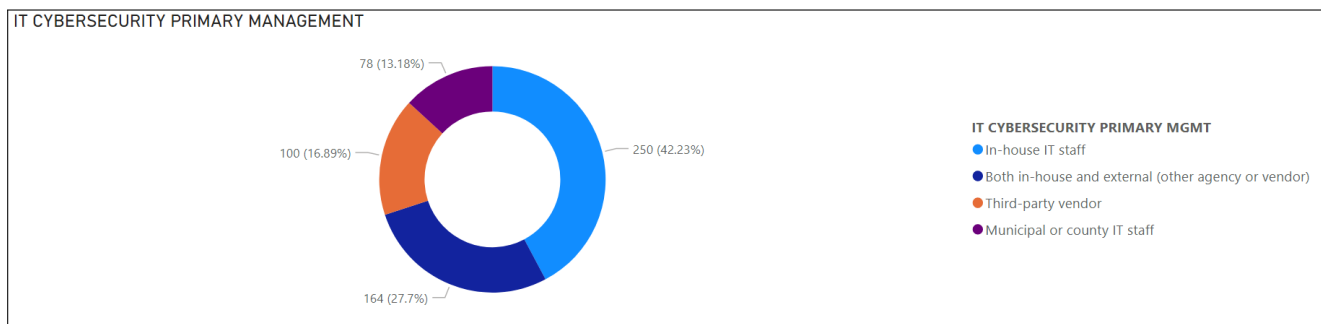


15.8% of systems reported having experienced 1 to 4 IT cybersecurity incidents in the last twelve months.

77.8% of systems reported no OT cybersecurity incidents in the last twelve months.

4.7% of systems reported having experienced 1 to 4 OT cybersecurity incidents in the last twelve months.

## IT and OT Management and Workforce

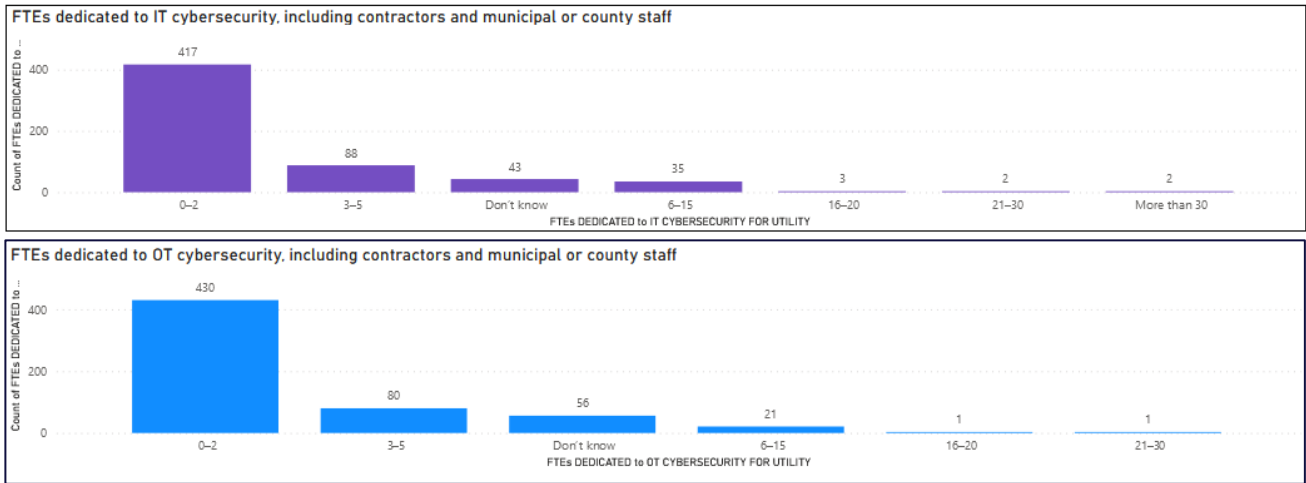


42% of utility IT cybersecurity is primarily managed by in-house IT staff. 27.7% of utility IT cybersecurity is primarily managed by both in-house and external vendors or other agencies. 16.89% of utility IT cybersecurity is primarily managed by third-party vendors. And 13.18% of utility IT cybersecurity is primarily managed by municipal or county IT staff.

48.47% of utility OT/ICS cybersecurity is primarily managed by in-house IT staff. 25.25% of utility OT/ICS cybersecurity is primarily managed by both in-house and external vendors or other agencies. 18.98% of utility OT/ICS cybersecurity is primarily managed by third-party vendors. And 7.29% of utility OT/ICS cybersecurity is primarily managed by municipal or county IT staff.

63.8% of respondents provided that their utility does not employ a Chief Information Security Officer (CISO) or equivalent. 21.9% of utilities have a CISO or equivalent. 8% of respondents noted that the role resides with their municipal or county government.

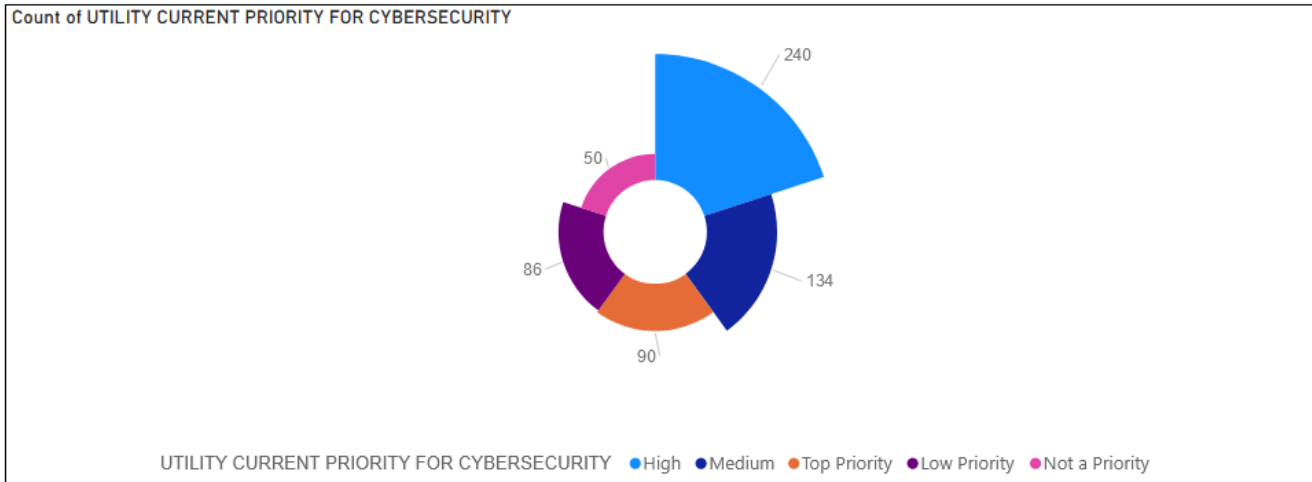
FTEs dedicated to cybersecurity include the following:



70.67% of respondents noted 0-2 FTEs dedicated to IT cybersecurity, and 73% of respondents noted 0-2 FTEs dedicated to OT cybersecurity. Additionally, the larger the utility the larger the increase in FTEs dedicated to cybersecurity.

## Current Focus on Cybersecurity as a Priority

| UTILITY CURRENT PRIORITY FOR CYBERSECURITY | 500 or fewer | 501-3,330 | 3,301-10,000 | 10,001-50,000 | 50,001-100,000 | 100,001-250,000 | Greater than 250,000 | Total      |
|--|--------------|-----------|--------------|---------------|----------------|-----------------|----------------------|------------|
| High                                       | 9            | 16        | 40           | 60            | 33             | 33              | 49                   | 240        |
| Low Priority                               | 33           | 27        | 8            | 7             | 5              | 4               | 2                    | 86         |
| Medium                                     | 1            | 16        | 32           | 22            | 26             | 11              | 7                    | 134        |
| Not a Priority                             | 34           | 8         | 7            |               |                |                 |                      | 50         |
| Top Priority                               | 5            | 14        | 8            | 18            | 10             | 9               |                      | 90         |
| <b>Total</b>                               | <b>1</b>     | <b>97</b> | <b>97</b>    | <b>85</b>     | <b>111</b>     | <b>59</b>       | <b>53</b>            | <b>600</b> |



55% of respondents ranked cybersecurity is a high or top priority. 22.3% consider cybersecurity a medium priority, while 22.6% - mainly systems serving 3,300 people or fewer- ranked cybersecurity a low priority or not a priority.

## Cybersecurity Resources Used in the Sector

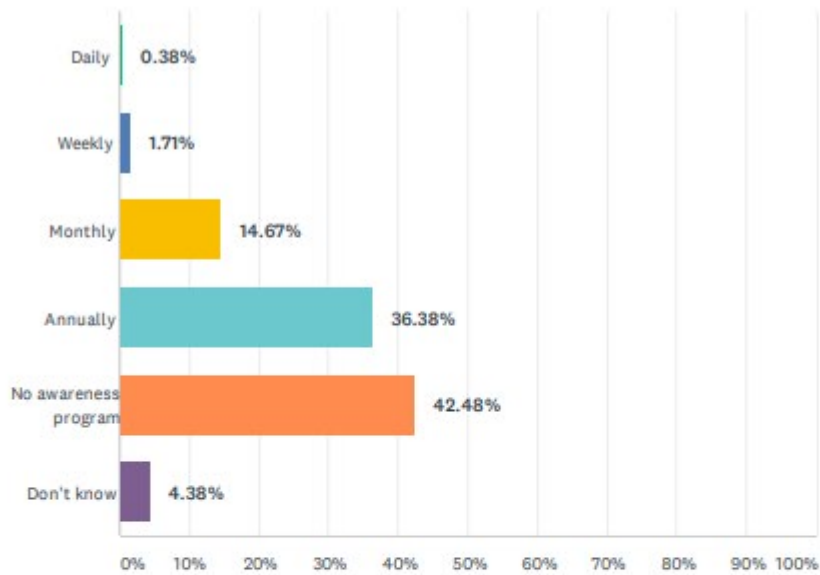
The top 5 cybersecurity resources used by utilities include the

- AWWA Cybersecurity Guidance (based on CSF)
- WaterISAC 15 Cybersecurity Fundamentals for Water and Wastewater Utilities
- NIST Cybersecurity Framework (CSF)
- DHS CISA Cybersecurity Assessment Tool (CSET) and other services
- NIST SP 800-82 Guide to Industrial Control Systems Security

Resources not covered by the survey include the U.S. Environmental Protection Agency's Cybersecurity Incident Action Checklist and its cybersecurity assessment program.

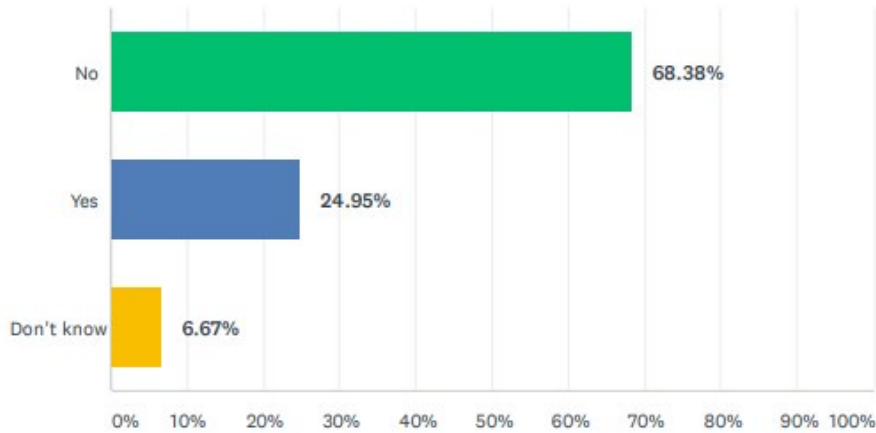
# Training

More than 50% of utilities conduct cybersecurity awareness training for utility staff:



| ANSWER CHOICES       | RESPONSES |            |
|----------------------|-----------|------------|
| Daily                | 0.38%     | 2          |
| Weekly               | 1.71%     | 9          |
| Monthly              | 14.67%    | 77         |
| Annually             | 36.38%    | 191        |
| No awareness program | 42.48%    | 223        |
| Don't know           | 4.38%     | 23         |
| <b>TOTAL</b>         |           | <b>525</b> |

The following provides that nearly 25% of utilities participate in cybersecurity-related tabletop exercises, mock drills, technology failure exercises or emergency management exercises:



| ANSWER CHOICES | RESPONSES |            |
|----------------|-----------|------------|
| No             | 68.38%    | 359        |
| Yes            | 24.95%    | 131        |
| Don't know     | 6.67%     | 35         |
| <b>TOTAL</b>   |           | <b>525</b> |

## Next Steps

Drinking water and wastewater utilities and the thousands of employees that run them are public health guardians and environmental protectors, treating drinking water to standards that meet state and federal regulations, ensuring wastewater treatment practices protect water bodies, and ensuring these vital services can continue in times of crisis.

On the whole, the sector recognizes the importance of investing in cybersecurity and adopting cybersecurity best practices. Many utilities are highly advanced, with expert IT and OT managers, keeping their devices, networks and consumers safe. Others, as shown in these results, require assistance to enhance their IT and OT cybersecurity. The sector itself also continues to support national cybersecurity efforts by collaborating with federal partners, developing its own sector-specific cybersecurity resources, and operating the Water Information Sharing and Analysis Center.

The challenges and needs outlined by respondents here offer guideposts for next steps by the Water and Wastewater Systems sector, Congress, federal agencies, and their partners.



**To:** The House Energy and Commerce Subcommittee on Environment, Manufacturing, & Critical Materials  
**From:** The National Association of Clean Water Agencies (NACWA) and the Water Environment Federation (WEF)  
**Date:** January 31, 2024  
**Subject:** Perspectives of Public Clean Water Agencies and Professionals on Ensuring the Cybersecurity of America's Water Sector Utilities

---

On behalf of the National Association of Clean Water Agencies (NACWA) and the Water Environment Federation (WEF), we thank you for holding today's hearing of the House Energy & Commerce's Environment, Manufacturing, & Critical Materials Subcommittee on Ensuring the Cybersecurity of America's Drinking Water Systems.

NACWA represents public wastewater and stormwater agencies of all sizes nationwide, with more than 350 public agency members. WEF serves as the not-for-profit technical and educational organization of 35,000 individual members and 75 affiliated Member Associations representing water quality professionals worldwide.

While NACWA and WEF primarily work on clean water policy and advocacy issues, we understand that today's hearing – although mainly focused on drinking water issues – may touch on topics and potential regulatory approaches that would impact clean water utilities. Accordingly, we submit these comments to provide our perspective on these issues as they relate to public clean water utilities. Our comments are not intended to provide any opinion or position on cybersecurity issues as they apply to drinking water utilities.

Properly treated and managed wastewater and stormwater are essential in protecting both public health and the environment. With more than 16,000 publicly owned treatment works (POTWs) throughout the nation that treat more than 75 percent of America's wastewater, public clean water agencies play a prominent role in protecting the public by treating billions of gallons of the nation's wastewater. To ensure continuity of treatment while cyber threats continue to target America's critical infrastructure, efforts must be made to provide public utilities with robust voluntary resources to better protect themselves from cyberattacks.

Many utilities have taken proactive steps to improve their cybersecurity, investing their limited ratepayer funds to protect their infrastructure and operations. NACWA and WEF are very appreciative of the extensive resources that already exist at the federal level:

- The Cybersecurity and Infrastructure Security Agency (CISA) provides free vulnerability scanning services for utilities and resources, such as guidance on



best practices, the Cyber Security Evaluation Tool, and vulnerability alerts and updates.

- The U.S. Environmental Protection Agency (EPA) provides free technical assistance and cybersecurity assessment resources.
- The National Institute of Standards and Technology (NIST) provides many best practice resources, including the NIST Cybersecurity Framework.

In addition to these resources, several water sector organizations have developed additional tools for utilities to better prepare against cyber threats:

- The Water Information Sharing and Analysis Center (WaterISAC), a non-profit organization comprised of water and wastewater utility managers and administrators, provides up-to-date alerts, information, and analysis specifically for the water sector and is managed by the Association of Metropolitan Water Agencies (AMWA).
- The American Water Works Association (AWWA) has developed a Cybersecurity Assessment Tool and Guidance, which assists water sector utility operators on how best to implement applicable cyber controls based on the NIST Cybersecurity Framework that can significantly reduce a utility's vulnerability to a cyberattack.

Congress can help support clean water agencies in their efforts to leverage existing resources and improve cybersecurity in a variety of ways, including:

- The Energy and Commerce Committee should act favorably on H.R.1367, the *Water System Threat Preparedness and Resilience Act of 2023*, to offset the cost of WaterISAC membership for eligible utilities and help water systems be more aware and prepared for cyberattacks.
- The American Water Works Association (AWWA) has developed a Cybersecurity Assessment Tool and Guidance, which assists water sector utility operators on how best to implement applicable cyber controls based on the NIST Cybersecurity Framework that can significantly reduce a utility's vulnerability to a cyberattack.

In addition, federal agencies should be encouraged to work with utilities and water sector associations to improve cybersecurity in a variety of ways that include:

- EPA, CISA, and WaterISAC should work with the vendors and contractors supplying equipment to the clean water sector to ensure that their products

and services are set up and maintained appropriately to ensure that they are secure, including communicating to and training utility staff on best practices.

- EPA and CISA should continue providing federal support to help prevent attacks through training, cybersecurity services, technical assessments, and pre-attack planning and continue providing an incident response to assist the sector in reducing the scale and duration of impacts if attacked. The agencies should consider collaborating with NACWA and WEF to develop additional guidance documents and resources to help clean water utilities understand and implement cybersecurity best practices.
- Speed, flexibility, and responsiveness are critical in the rapidly evolving world of cybersecurity. Encouraging public utilities to use existing tools, resources, and best practices will improve resilience to cyber-attacks faster than cumbersome regulatory structures enacted by federal agencies or a third-party entity.

Lastly, as many clean water utilities are already fully engaged in improving and maintaining existing cybersecurity protocols, NACWA and WEF firmly believe that allowing clean water utilities to improve their cybersecurity voluntarily, rather than implementing a direct or third-party quasi-regulatory system, is the best approach for wastewater utilities for a variety of reasons that include:

- Developing a regulatory approach for clean water utilities, such as third-party oversight within EPA, will take years, and a one-size-fits-all approach to cybersecurity will not provide for innovative, collaborative, cross-sector approaches for developing, designing, and implementing successful cybersecurity programs in the sector.
- Clean water utilities can leverage existing resources immediately rather than waiting to see what regulations are finalized to avoid taking measures that may be duplicative or not meet the requirements of potential regulations.
- Since clean water utilities may be part of city or county government that are already subject to state cybersecurity requirements, a voluntary approach to cybersecurity allows flexibility for utilities to develop cybersecurity approaches and practices that meet their needs and that can be developed in line with best practices from other brother/sister utilities and city/county departments.

NACWA and WEF thank the Subcommittee for the opportunity to submit comments. We look forward to working with your members on federal policies that maintain and provide clean water utilities with resources that will provide speed, flexibility, and responsiveness to adapt to

Perspectives of Public Clean Water Agencies and Professionals on Ensuring the Cybersecurity of America's Water Sector Utilities

January 31, 2024

Page 4 of 4

cybersecurity threats. Encouraging public utilities to use existing tools, resources, and best practices will improve resilience to cyberattacks.

If you have any questions, please have your staff contact Matt McKenna ([mmckenna@nacwa.org](mailto:mmckenna@nacwa.org)) or Steve Dye ([sdye@wef.org](mailto:sdye@wef.org)).



# U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-24-09

January 9, 2024

## **FINAL REPORT**

# **CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector**





# OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | [www.oig.dhs.gov](http://www.oig.dhs.gov)

January 9, 2024

MEMORANDUM FOR: Jen Easterly  
Director  
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D.  
Inspector General

SUBJECT: *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector*

**JOSEPH V  
CUFFARI**

Digitally signed by JOSEPH V CUFFARI  
Date: 2024.01.09 16:50:48 -0700

Attached for your action is our final report, *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving CISA's external collaboration and internal coordination within the Water and Wastewater Sector. Your office concurred with all three recommendations.

Based on information provided in your response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to [OIGAuditsFollowup@oig.dhs.gov](mailto:OIGAuditsFollowup@oig.dhs.gov).

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



# DHS OIG HIGHLIGHTS

## CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector

January 9, 2024

### Why We Did This Audit

The Department of Homeland Security is responsible for overseeing domestic critical infrastructure protection efforts. Recent cyber intrusions highlight the need for a resilient Water and Wastewater Systems Sector. Our audit objective was to determine the extent of DHS' coordinated efforts to manage risks and mitigate against cybersecurity threats to critical water and wastewater infrastructure while seeking opportunities and capabilities to increase the infrastructure's resiliency.

### What We Recommend

We made three recommendations to improve CISA's external collaboration and internal coordination.

**For Further Information:**

Contact our Office of Public Affairs at (202) 981-6000, or email us at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).

### What We Found

The Cybersecurity and Infrastructure Security Agency (CISA) had extensive products and services to manage risks and mitigate cybersecurity threats to critical water and wastewater infrastructure and increase its resiliency. However, CISA did not consistently collaborate with the Environmental Protection Agency and the Water and Wastewater Systems Sector to leverage and integrate its cybersecurity expertise with stakeholders' water expertise. This occurred because CISA did not have a Memorandum of Understanding with the Environmental Protection Agency documenting roles, responsibilities, and collaboration mechanisms. CISA also lacked policies and procedures regarding collaboration with the Environmental Protection Agency and other external stakeholders.

In addition, CISA did not coordinate effectively between its divisions on sharing of critical information. This occurred because CISA did not have agency-wide policies and procedures related to internal coordination.

Finally, CISA lacked a strategic plan during the period of our audit that identified its goals and objectives. However, in September 2022, CISA released its first strategic plan.

Without consistent collaboration with external stakeholders, effective internal coordination, and a strategic plan, CISA was limited in ensuring cyber risks were appropriately communicated to stakeholders and that stakeholders were aware of CISA's products and services.

### CISA Response

CISA concurred with all three recommendations.



# OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

## Table of Contents

|  |    |
|--|----|
| Background .....   | 1  |
| Results of Audit .....   | 4  |
| CISA Offered Extensive Cybersecurity Products and Services But Did Not Consistently Collaborate with External Water Stakeholders ..... | 4  |
| CISA Did Not Coordinate Effectively Between Divisions .....  | 8  |
| CISA Lacked a Strategic Plan Documenting Its Goals and Metrics for Strengthening Cybersecurity and Resiliency.....                     | 9  |
| Conclusion.....  | 10 |
| Recommendations.....   | 10 |
| Management Comments and OIG Analysis.....  | 11 |
| Appendix A: Objective, Scope, and Methodology.....   | 13 |
| DHS OIG’s Access to DHS Information.....   | 14 |
| Appendix B: CISA Comments to the Draft Report.....   | 15 |
| Appendix C: Sixteen Critical Infrastructure Sectors and Sector Risk Management Agencies .....  | 19 |
| Appendix D: Report Distribution.....   | 20 |

## Abbreviations

|        |  |
|--------|--|
| AOP    | Annual Operating Plan                            |
| CISA   | Cybersecurity and Infrastructure Security Agency |
| EPA    | Environmental Protection Agency                  |
| GAO    | U.S. Government Accountability Office            |
| PPD-21 | Presidential Policy Directive-21                 |
| SCC    | Sector Coordinating Council                      |
| SPP    | Office of Strategy, Policy, and Plans            |
| SRMA   | Sector Risk Management Agency                    |



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

### Background

Cybersecurity is an area with an increasing number of risks, threats, and vulnerabilities. Recent cyber intrusions have highlighted the need for a resilient Water and Wastewater Systems Sector (Water Sector). For example, an unidentified hacker allegedly tried to gain unauthorized access to systems to poison a San Francisco Bay area water treatment plant in January 2021.<sup>1</sup> Additionally, in March 2021, a former employee of a Kansas public water system was indicted for remotely accessing a protected computer without authorization.<sup>2</sup>

The Water Sector is composed of infrastructure of varying sizes and ownership types. Water utilities can be owned and managed by a municipality, county, independent district or authority, private company, or not-for-profit water association. There are approximately 50,000 community water systems in the United States. In addition, there are more than 16,000 publicly owned wastewater treatment systems of various sizes serving the country.

The Water Sector is one of 16 critical infrastructure sectors identified in the February 2013 *Presidential Policy Directive-21* (PPD-21).<sup>3</sup> Each critical infrastructure sector has unique characteristics, operating models, and risk profiles. The Environmental Protection Agency (EPA) is the lead agency, or Sector Risk Management Agency (SRMA),<sup>4</sup> for the Water Sector. As SRMA, EPA's responsibilities include:

- coordinating with the Department of Homeland Security — more specifically, the Cybersecurity and Infrastructure Security Agency (CISA) — and collaborating with critical infrastructure owners and operators; independent regulatory agencies; and state, local, tribal, and territorial entities;
- serving as the day-to-day Federal interface for the sector; and
- providing, supporting, or facilitating technical assistance to the sector to identify vulnerabilities and help mitigate incidents.

---

<sup>1</sup> Kevin Collier, *50,000 security disasters waiting to happen: The problem of America's water supplies*, NBC News (June 17, 2021), <https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206>.

<sup>2</sup> U.S. Attorney's Office, District of Kansas, *Indictment: Kansas Man Indicted For Tampering With A Public Water System*, Department of Justice (Mar. 31, 2021), <https://www.justice.gov/usao-ks/pr/indictment-kansas-man-indicted-tampering-public-water-system>.

<sup>3</sup> [Presidential Policy Directive \(PPD\) 21: Critical Infrastructure Security and Resilience | CISA](#).

<sup>4</sup> The *National Defense Authorization Act for FY 2021* redefined Sector-Specific Agencies as Sector Risk Management Agencies.





## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

Each of the 16 critical infrastructure sectors (see table in Appendix C) also has a Sector Coordinating Council (SCC). The Water Sector Coordinating Council (Water SCC) is the advisory body comprising organizations such as the American Water Works Association.<sup>5</sup> The Water Information Sharing Analysis Center, established in coordination with EPA, is the information-sharing arm for the Water SCC and the only all-threats security information source for the Water Sector.

CISA is the lead Federal agency responsible for overseeing domestic critical infrastructure protection efforts. CISA's mission is to lead the national effort to understand, manage, and reduce risks to cyber and physical infrastructure. CISA is organized into six main divisions (see Table 1). In addition to the six divisions, CISA has an Office of Strategy, Policy, and Plans (SPP) that leads and enables mission execution through strategic planning, national policy coordination, internal governance implementation, and enterprise-wide process improvements.

---

<sup>5</sup> The American Water Works Association has 51,000 members and includes more than 4,300 utilities that supply water to roughly 80 percent of the nation.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

**Table 1. CISA’s Six Divisions and Key Functions**

| DIVISION                                 | KEY FUNCTIONS  |
|--|--|
| <b>Cybersecurity Division*</b>           | Leads the effort to protect the Federal and civilian government networks and to collaborate with the private sector to increase the security of critical networks through capability delivery, threat hunting, vulnerability management, and cyber defense training and education. |
| <b>National Risk Management Center*</b>  | Works with the critical infrastructure community to identify and analyze the most significant cyber and physical risks to our Nation, and strategically manage resiliency and security efforts.  |
| <b>Infrastructure Security Division*</b> | Coordinates and collaborates across government and the private sector; conducts and facilitates vulnerability and consequence assessments to help critical infrastructure owners and operators understand and address risks.   |
| <b>Integrated Operations Division*</b>   | Provides 24/7/365 situational awareness and near-real-time operational reporting; conducts all-source intelligence analysis and delivers cyber and physical vulnerability assessments.   |
| <b>Stakeholder Engagement Division*</b>  | Develops partnerships, facilitates dialogue, convenes stakeholders, and promotes awareness to help CISA achieve a secure and resilient infrastructure.   |
| <b>Emergency Communications Division</b> | Supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient.  |

Source: DHS Office of Inspector General analysis of CISA website at [www.cisa.gov](http://www.cisa.gov)

\* Reflects the five divisions DHS OIG identified as having key functions related to cybersecurity of critical infrastructure, including the Water Sector.

CISA supports EPA in helping to reduce the risk of cyber threats and increasing the Water Sector’s resiliency. Other DHS components, such as the Federal Emergency Management Agency, the Office of Intelligence and Analysis, and the Science and Technology Directorate, also support the Water Sector through activities to increase cyber resilience, such as developing exercises and sharing risk and threat information.

We conducted this audit to determine the extent of DHS’ coordinated efforts to manage risks and mitigate against cybersecurity threats to critical water and wastewater infrastructure while seeking opportunities and capabilities to increase the infrastructure’s resiliency. The scope of our audit was efforts during fiscal years 2019 through 2022.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

### Results of Audit

During this audit, CISA had extensive products and services available to its stakeholders to manage risks and mitigate cybersecurity threats to critical water and wastewater infrastructure to increase its resiliency. However, CISA did not consistently collaborate with EPA and the Water Sector to leverage and integrate its cybersecurity expertise with stakeholders' water expertise. This occurred because CISA did not have a written agreement with EPA regarding its interagency collaboration or policies and procedures to ensure appropriate collaboration<sup>6</sup> with EPA and other Water Sector stakeholders.

In addition, CISA did not coordinate effectively between its divisions on sharing of critical information. This occurred because CISA did not have agency-wide policies and procedures related to internal coordination.

Finally, CISA lacked a strategic plan during the period of our audit that identified its goals and objectives. However, in September 2022, CISA released its first strategic plan.

Without consistent collaboration with external stakeholders, effective internal coordination, and a Strategic Plan, CISA was limited in ensuring cyber risks were appropriately communicated to stakeholders and that stakeholders were aware of CISA's products and services to help improve resiliency against cyber threats.

### **CISA Offered Extensive Cybersecurity Products and Services, But Did Not Consistently Collaborate with External Water Stakeholders**

We found that CISA had an extensive portfolio of products and services to help the Water Sector manage risks and mitigate cybersecurity threats to critical infrastructure to increase its resiliency. However, CISA did not consistently collaborate with EPA and other Water Sector stakeholders to leverage and integrate its cybersecurity expertise with stakeholders' water expertise.

#### **Cybersecurity Products and Services Offered by CISA**

During our audit, we determined CISA has an extensive portfolio of available products and services to help the Water Sector manage risks and mitigate cybersecurity threats to its infrastructure and to increase its resiliency. These services include:

- **Vulnerability Scanning**: Non-intrusive checks to determine potential vulnerabilities and configuration weaknesses.

---

<sup>6</sup> PPD-21 defines "collaboration" as the process of working together to achieve shared goals.



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- Web Application Scanning: Non-intrusive checks of publicly accessible web applications to determine vulnerabilities, bugs, and weak configurations.
- Cyber Resilience Review: Interview-based assessment that measures a public water system's operational and cybersecurity practices and the capabilities and capacities to plan, manage, measure, and define cybersecurity across 10 domains.
- CISA Tabletop Exercise Packages: A comprehensive set of resources designed to assist stakeholders in conducting their own exercises. The packages include pre-built templates for exercise planning, execution, and follow-up.

### **CISA Did Not Consistently Collaborate with EPA and Other External Water Sector Stakeholders**

CISA did not consistently collaborate with EPA and other external Water Sector stakeholders to leverage and integrate its cybersecurity expertise with stakeholders' water expertise. The *Cybersecurity and Infrastructure Security Agency Act of 2018*<sup>7</sup> (CISA Act) requires CISA to develop and implement a mechanism for active and frequent collaboration with SRMAs — in this case, EPA. PPD-21 clarifies critical infrastructure-related functions, roles, and responsibilities across the Federal Government and calls for enhancing overall coordination and collaboration.

According to PPD-21, DHS' coordination roles and responsibilities include:

- identifying and prioritizing critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SRMAs and other Federal departments and agencies; and
- conducting comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SRMAs and in collaboration with State, Local, Tribal, and Territorial entities and critical infrastructure owners and operators.

According to EPA water sector officials, EPA was mostly satisfied with its collaboration with CISA, but there were instances in which CISA did not communicate well with EPA. A senior official with EPA's Office of Water stated that, at times, a CISA division would identify Water Sector projects without coordinating with EPA as to the purpose or need for the projects. The same official suggested CISA could improve its performance by engaging EPA more directly in the identification and organization of sector-specific projects. This would benefit the projects in terms of substance and enhance related communication with the Water Sector. CISA officials acknowledged the need to improve its collaboration with EPA and produce better products for the Water Sector.

---

<sup>7</sup> Public Law 115-278, (codified as 6 U.S.C. § 652(c)(6)).



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

The inconsistent collaboration, as cited by the EPA official, occurred because CISA had not established formal mechanisms for its interactions with EPA, including (1) a written Memorandum of Understanding with EPA and (2) internal policies and procedures regarding its collaboration. Specifically, CISA had not documented its relationship with EPA in the form of a written Memorandum of Understanding that defined each agency's roles and responsibilities and the mechanisms for collaboration. According to the U.S. Government Accountability Office (GAO), agencies can strengthen their commitment to work collaboratively by articulating their agreements in formal documents, such as Memorandums of Understanding. Additionally, CISA did not have established policies and processes for its Water Sector Liaison's role, how divisions should coordinate their communication with EPA, when CISA should collaborate with EPA to share information with the Water Sector, what information should be shared, or how often information should be shared. CISA's former acting Water Sector Liaison said CISA used PPD-21 and the CISA Act as guiding documents and authorities to define the Water Sector Liaison role. However, we found that PPD-21 and the CISA Act only broadly define the role and do not prescribe a process for CISA to support the SRMA, the frequency of collaboration, or what information should be shared.

We also determined there was ineffective collaboration between CISA and other Water Sector stakeholders, such as the SCC. Executive Order 13636 *Improving Critical Infrastructure Cybersecurity*<sup>8</sup> directs DHS to establish a consultative process to coordinate improvements to critical infrastructure cybersecurity. Executive Order 13636 expressly states DHS should consider the advice of the SCC, critical infrastructure owners, and other entities, in addition to the SRMA. The *Water and Wastewater Systems Sector-Specific Plan 2015*<sup>9</sup> recognizes the Water SCC as a key link between Federal Government agencies and Water Sector owners and operators.

Based on our meetings with the Water SCC, a number of specific concerns were raised by Water SCC officials, such as:

- **Direct Engagement with CISA:** Officials said they would benefit from increased, direct engagement with CISA. One Water SCC official indicated the relationship between CISA and EPA led to filtering of messages from CISA to the Water SCC and vice versa. In the official's view, this filtering of information resulted in CISA not necessarily receiving the most appropriate responses from the Water SCC. A CISA official acknowledged that CISA did not have consistent communication with the Water SCC and said the Water SCC was supposed to report to EPA, but Water SCC officials noted a lack of clear guidance

---

<sup>8</sup> *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*, The White House, Office of the Press Secretary, February 12, 2013.

<sup>9</sup> The *Water and Wastewater Systems Sector-Specific Plan 2015* addresses risk-based critical infrastructure protection strategies for drinking water and wastewater utilities and describes processes and activities to enhance the security and resilience of the sector's infrastructure.



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

regarding their ability to elevate concerns directly to CISA versus EPA.

- **Understanding of CISA's Products and Services:** Officials said they often did not have a good understanding of CISA's products and services, which limited their ability to communicate what was available to their member organizations and resulted in potential missed opportunities to mitigate cyber risks.
- **Participation in Development of CISA's Products and Services:** Officials indicated CISA did not include them early enough in its process of developing products and services. They stated that by the time Water Sector stakeholders were included, it was too late to incorporate their feedback, despite its substantive nature. According to these same officials, this resulted in CISA products and services that only partially met the needs of the Water Sector or were not user-friendly. One American Water Works Association official said some tools and guidance were too technical and hard to understand for the average water utility system employee.
- **Lack of Water Industry Experience:** Officials cited the lack of a full-time Water Sector Liaison within CISA with a clearly defined role and water industry expertise as a factor in collaboration challenges. They indicated that lack of an effective Water Sector Liaison caused difficulties when communicating about complex water sector security issues. CISA has addressed this concern by recently hiring a full-time Water Sector Liaison who has more than 20 years of water industry experience.

These collaboration issues occurred because CISA did not have policies and procedures governing direct interaction with Water Sector stakeholders to manage risks and mitigate cybersecurity threats. This is inconsistent with the external coordination requirements of Executive Order 13636, as stated above, and GAO's *Standards for Internal Control in the Federal Government*,<sup>10</sup> which states that management should communicate quality information externally through reporting lines so that external parties can help the entity achieve its objectives and address related risks.

Without consistent collaboration with external stakeholders, CISA was limited in ensuring cyber risks were appropriately communicated to stakeholders and that stakeholders were aware of CISA's products and services to help improve resiliency against cyber threats.

---

<sup>10</sup> *Standards for Internal Control in the Federal Government* (GAO-14-704G), September 2014, <https://www.gao.gov/assets/gao-14-704g.pdf>.



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

### CISA Did Not Coordinate Effectively Between Divisions

According to the CISA Act,<sup>11</sup> the CISA Director shall maintain and use mechanisms for regular and ongoing consultation and coordination among CISA divisions. GAO has also long maintained that establishing compatible policies, procedures, and other means to operate across agency boundaries is a best practice to enhance and sustain collaborative efforts.<sup>12</sup> GAO's *Standards for Internal Control in the Federal Government* further state that management should internally communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives and addressing risks.

CISA's internal coordination among its divisions was ineffective. While some degree of coordination exists between divisions, officials could not articulate how they coordinated among the divisions. For example, a National Risk Management Center official said they coordinate with the Cybersecurity Division, the Stakeholder Engagement Division, and the Infrastructure Security Division as needed; however, the official could not identify or describe the specifics of what information was shared, how it was shared, and with whom. An official also said that Cybersecurity Division coordinates with the Integrated Operations Division but could not provide a clear description of what type of communication was shared as well.

Further, we found that the Stakeholder Engagement Division was not always notified when other CISA divisions communicated with EPA, and there was no indication that the Stakeholder Engagement Division coordinated or tracked the information shared by the other divisions. As part of its mission, the Stakeholder Engagement Division is supposed to coordinate stakeholder engagement and partnerships and focus on activities that support CISA's unified, customer-centric approach. Thus, the Stakeholder Engagement Division should be the central point of contact for CISA's communication with stakeholders. The Stakeholder Engagement Division has developed a draft of the sector liaison operating procedures that an official said will be the overarching guidance for all eight sectors for which DHS is not the SRMA. While this is a good start, we found that the draft procedures contained mainly administrative duties, were not sector-specific, and did not directly discuss the process for determining who should have access to different types of information.

These coordination issues occurred because CISA lacked written policies and procedures related to internal coordination and need-to-know protocols. Moreover, according to CISA SPP officials, the agency did not have an agency-wide requirement for divisions to document policies and procedures. They said they would only get involved to document policies if programs or services crossed two or more divisions and rose to the enterprise level. A CISA SPP official acknowledged

<sup>11</sup> Public Law 115-278, (codified as 6 U.S.C. § 652(c)(7)).

<sup>12</sup> *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies* (GAO-06-15), October 2005, <https://www.gao.gov/assets/gao-06-15.pdf>.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

that it is in the process of developing policies and has a backlog of over 200 policy needs, including some covering cross-divisional functions.

We found that there were no agency-wide policies and procedures and only two of the five divisions that support the Water Sector provided division-level policies related to coordination. The Integrated Operations Division's documentation provided detailed policies its staff used in daily communication and coordination activities. However, an official acknowledged that the Integrated Operations Division could better document processes, such as how to engage regions and headquarters.

Without clear written guidance, CISA cannot ensure effective internal coordination which undermines its mission performance, particularly as it relates to the Water Sector.

### **CISA Lacked a Strategic Plan Documenting Its Goals and Metrics for Strengthening Cybersecurity and Resiliency**

During the period of our audit, CISA lacked a strategic plan that documented CISA's overall goals and the metrics to strengthen cybersecurity and resiliency of the Water Sector. CISA was established as an agency in November 2018 with passage of the *CISA Act*, which required that CISA's Director develop, coordinate, and implement comprehensive strategic plans for the activities of the agency (Sec. 2202(c)(8)(A)). This work had not yet been completed during the period of our audit.

However, in September 2022, CISA released its first strategic plan, *CISA Strategic Plan 2023-2025*. The Strategic Plan establishes four goals, including:

1. **Cyber Defense:** Spearhead the national effort to ensure defense and resilience of cyberspace.
2. **Risk Reduction and Resilience:** Reduce risks to, and strengthen resilience of, America's critical infrastructure.
3. **Operational Collaboration:** Strengthen whole-of-nation operational collaboration and information sharing.
4. **Agency Unification:** Unify as One CISA through integrated functions, capabilities, and workforce.

The Strategic Plan identifies multiple objectives supporting each of these goals. Additionally, the Strategic Plan identifies its measurement approach for evaluating progress for each of the objectives. CISA is developing specific measures of performance and effectiveness, which will be





## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

defined in future annual operating plans. Implementation of its strategic plan and annual operating plans should allow better evaluation of program success.

Of note, the Strategic Plan identifies “Operational Collaboration” as one of its four agency-wide goals. The goal’s five objectives relate to strengthening collaboration with external stakeholders and internally within CISA. Focusing on these objectives should help address the external collaboration and internal coordination issues identified in this report. The objectives include:

- Optimizing collaborative planning and implementation of stakeholder engagements and partnership activities (External and Internal)
- Fully integrating regional offices into CISA’s operational coordination (Internal)
- Streamlining stakeholder access to and use of appropriate CISA programs, products, and services (External)
- Enhancing information sharing with CISA’s partnership base (External)
- Increasing integration of stakeholder insights to inform CISA product development and mission delivery (External and Internal)

Because CISA has now issued its Strategic Plan and is moving forward with development of annual operating plans, we have no recommendations in this area.

### Conclusion

CISA offered an extensive portfolio of products and services to manage risks and mitigate cybersecurity threats and increase resilience of the Water Sector infrastructure. However, without consistent collaboration with external stakeholders, effective internal coordination, and a Strategic Plan, CISA was limited in ensuring cyber risks were appropriately communicated to stakeholders and that stakeholders were aware of CISA’s products and services to help improve resiliency against cyber threats.

### Recommendations

**Recommendation 1:** We recommend the CISA Director establish and implement a written Memorandum of Understanding with EPA to fully document each agency’s roles and responsibilities and mechanisms for collaboration.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

**Recommendation 2:** We recommend the CISA Director develop and implement comprehensive policies and procedures regarding its collaboration with EPA and other Water and Wastewater Systems Sector stakeholders. These policies and procedures should address:

- the Water Sector Liaison’s roles and responsibilities;
- what information should be shared with stakeholders;
- how often and when divisions should coordinate their communications; and
- how best to facilitate information sharing about cyber threats, vulnerabilities, incidents, potential protective measures, and best practices, in both routine and urgent circumstances.

**Recommendation 3:** We recommend the CISA Director have an agency-wide requirement to develop and implement standard operating procedures to improve regular communication among CISA divisions relevant to the Water and Wastewater Sector or other critical infrastructure Sectors and share that information and updates on projects, decisions, and lead roles and responsibilities related to the Water and Wastewater Systems Sector and other sectors as appropriate.

### Management Comments and OIG Analysis

CISA provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments from CISA on the draft report, and we took the component’s suggested changes into consideration. CISA concurred with all three recommendations, which we consider open and resolved. A summary of CISA’s response and our analysis follows.

**CISA Response to Recommendation 1:** Concur. CISA’s Stakeholder Engagement Division and SPP will coordinate with EPA to document and define its interagency partnership and their respective roles and responsibilities. CISA’s Stakeholder Engagement Division will document these items in the Memorandum of Understanding with EPA. Estimated Completion Date: October 31, 2024.

**OIG Analysis:** These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when CISA provides the Memorandum of Understanding with EPA that documents their clearly defined roles and responsibilities in collaborating with one another.

**CISA Response to Recommendation 2:** Concur. After CISA completes the Memorandum of Understanding with EPA, CISA’s Stakeholder Engagement Division and SPP will develop and implement policies and procedures regarding its collaboration with EPA and the Water Sector. Estimated Completion Date: May 30, 2025.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

**OIG Analysis:** These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when CISA provides the documented policies and procedures. Those policies and procedures should address the Water Sector Liaison's roles and responsibilities and CISA's engagement with EPA and other Water Sector stakeholders about cyber threats, vulnerabilities, incidents, potential protective measures, and best practices, in both routine and urgent circumstances.

**CISA Response to Recommendation 3:** Concur. For agency-wide communication and coordination, CISA's Infrastructure Security Division and Water Sector Liaison are coordinating through the Water and Wastewater Cybersecurity Engagement Working Group, and CISA's Water and Wastewater Community of Interest group. Additionally, CISA's Stakeholder Engagement Division will coordinate with other CISA Divisions to document an agency-wide requirement to develop and implement standard operating procedures on communication and information sharing. However, CISA is waiting for updates to the SRMA's role and responsibilities and the expectations for the SRMA's engagement with other Federal agencies in PPD- 21. CISA will then incorporate these changes and update its FY 2025 Annual Operating Plan with the agency-wide requirement. Estimated Completion Date: September 30, 2025.

**OIG Analysis:** These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when CISA provides documentation to show its coordination work through the Water and Wastewater Cybersecurity Engagement Working Group and CISA's Water and Wastewater Community of Interest group. In addition, the recommendation will remain open pending the receipt of an FY 2025 Annual Operating Plan that includes the agency-wide requirement to develop and implement standard operating procedures on communication and information sharing.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

### Appendix A: Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We audited DHS' coordinated efforts to protect, strengthen, and maintain critical water and wastewater infrastructure from FY 2019 through FY 2022. Our objective was to determine the extent of DHS' coordinated efforts to manage risks and mitigate against cybersecurity threats to critical water and wastewater infrastructure while seeking opportunities and capabilities to increase the infrastructure's resiliency.

To perform our audit, we reviewed relevant prior OIG and GAO reports including GAO's *Standards for Internal Control in the Federal Government (GAO-14-704G)*; *Results-Oriented Government – Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies (GAO-06-15)*; and *Managing for Results – Key Considerations for Implementing Interagency Collaborative Mechanisms (GAO-12-1022)*; along with other media reports and testimonies. We also reviewed applicable Federal laws, Executive Orders, component policies and procedures, and other water and wastewater sector guidance; evaluated DHS' internal control environment; and assessed the risks that our audit procedures or findings may be improper or incomplete.

We interviewed relevant officials within DHS including officials with FEMA's Grants Program Directorate and National Exercise Division; officials within the Office of Intelligence and Analysis' Cyber Mission Center; and officials within the Science and Technology Directorate. We also interviewed officials within five of the six CISA divisions including the Cybersecurity Division, Infrastructure Security Division, Integrated Operations Division, National Risk Management Center, and Stakeholder Engagement Division. In addition, we interviewed officials with CISA's Office of Strategy, Policy, and Plans. We did not interview officials from the Emergency Communications Division; we did not deem that division's work relevant to our audit objective.

We also interviewed officials outside of DHS including officials from EPA (the SRMA for the Water Sector) to discuss similar prior or ongoing audits and to corroborate information received from the DHS components, entities, and divisions mentioned above. We also interviewed officials from the Water Information Sharing and Analysis Center, Water SCC, and American Water Works Association. Lastly, we met with GAO officials to discuss our audit and to keep each other informed of any key information and potential issues so as not to duplicate work.



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

We did not conduct data reliability analyses of systems or data because the audit did not require the use of DHS systems or data.

We assessed DHS' internal controls related to our audit objective. Specifically, we assessed the design, implementation, and operating effectiveness of the controls in place to determine whether DHS' collaborative process was operating in accordance with laws and regulations and operating effectively and efficiently. Our assessment disclosed that the overall internal control risk was high. These weaknesses are discussed in the body of this report. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

We conducted this audit between May 2022 and April 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424, as amended, and according to 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.

### **DHS OIG's Access to DHS Information**

During this audit, CISA provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security


### Appendix B: CISA Comments to the Draft Report



U.S. Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency  
Office of the Director  
Washington, DC 20528

November 29, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.  
Inspector General

FROM: Jen Easterly   
Director  
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "CISA Needs to  
Improve Its Collaboration to Enhance Cyber Resiliency in the  
Water and Wastewater Sector"  
(Project No. 22-032-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA leadership is pleased to note OIG's positive recognition of our efforts to support Sector Risk Management Agencies (SRMAs) implementation of their statutory responsibilities, including our work to improve coordination with critical infrastructure sector partners through focused information sharing initiatives. OIG also acknowledged that several CISA products and services are actively being used by partners within the Water and Wastewater Sector, including vulnerability scanning, Cyber Resilience Reviews, and CISA Tabletop Exercise Packages.

However, while the scope of the audit covers fiscal years (FY) 2019 through 2022, it is important to note that CISA continued to improve collaboration with the Environmental Protection Agency (EPA) and Water Sector Coordinating Council (WSCC) during FY 2023. Specifically, CISA's FY 2023 priority initiatives included improvement of the support provided to, and coordination conducted with, the Water and Wastewater Sector. Accordingly, activities undertaken to implement CISA's FY 2023 priority initiatives resulted in qualitative improvements, such as CISA onboarding a Water and Wastewater Sector Liaison in December 2022, who has more than 20 years of experience working directly with partners across the sector. This liaison currently conducts four standing calls each month with EPA partners, in addition to conducting numerous other engagements with partners across the sector, and also instituted a cross-Division CISA Water and Wastewater Community of Interest group with over 50 members from all six



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

CISA Divisions to improve coordination in sector engagements and ensure that CISA is speaking with a unified voice in our engagements with the EPA, the WSCC, and other water sector partners.

In FY 2023, CISA Stakeholder Engagement Division (SED) also coordinated with EPA, the WSCC, and the Association of State Drinking Water Administrators to launch an awareness campaign, and in September 2023 developed a “co-branded” fact sheet on CISA’s free cyber vulnerability scanning service for water utilities.<sup>1</sup> As a direct result of this joint effort, Water and Wastewater Sector partner enrollment in CISA’s vulnerability scanning service increased by 30 percent in less than six months.

CISA remains committed to fulfilling our role as the SRMA for eight of the nation’s 16 critical infrastructure sectors, as defined in the “NIPP 2013: Partnering for Critical Infrastructure Security and Resilience,” dated February 2013 (National Plan),<sup>2</sup> and clarified in Section 9002 of the National Defense Authorization Act for FY 2021.<sup>3</sup> CISA will continue working with partners across sectors to sustain and strengthen collaborative security and resilience efforts.

The draft report contained three recommendations with which CISA concurs. Enclosed find our detailed response to each recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG’s consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Enclosure

---

<sup>1</sup> <https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities>

<sup>2</sup> <https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan>

<sup>3</sup> Section 9002 of Pub Law No. 116-283, <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>



## OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

---

### Enclosure: Management Response to Recommendations Contained in OIG 22-032-AUD-DHS

OIG recommended that the CISA Director:

**Recommendation 1:** Establish and implement a written Memorandum of Understanding [MOU] with EPA to fully document each agency's roles and responsibilities and mechanisms for collaboration.

**Response:** Concur. CISA's (SED), in coordination with the CISA Office of Strategy, Policy, and Plans (SPP), will coordinate with EPA to document the interagency partnership established in FY 2023, and further define agency roles and responsibilities. CISA's SED will formalize these standard operating procedures in a MOU with EPA. Estimated Completion Date (ECD): October 31, 2024.

**Recommendation 2:** Develop and implement comprehensive policies and procedures regarding its collaboration with EPA and other Water and Wastewater Systems Sector stakeholders. These policies and procedures should address:

- the Water Sector Liaison's roles and responsibilities;
- what information should be shared with stakeholders;
- how often and when divisions should coordinate their communications; and
- how best to facilitate information sharing about cyber threats, vulnerabilities, incidents, potential protective measures, and best practices, in both routine and urgent circumstances.

**Response:** Concur. Once CISA's SED establishes the MOU to documenting the interagency partnership with EPA by October 2024, CISA's SED and SPP will develop and implement comprehensive policies and procedures regarding collaboration with EPA and other Water and Wastewater Systems Sector stakeholders, to include the elements identified in this recommendation. ECD: May 30, 2025.

**Recommendation 3:** Have an agency-wide requirement to develop and implement standard operating procedures to improve regular communication among CISA divisions relevant to the Water and Wastewater Sector or other critical infrastructure Sectors and share that information and updates on projects, decisions, and lead roles and responsibilities related to the Water and Wastewater Systems Sector and other sectors as appropriate.

**Response:** Concur. CISA's Infrastructure Security Division (ISD) and the Water and Wastewater Sector Liaison are currently addressing agency-wide communication and coordination through the Water and Wastewater Cybersecurity Engagement Working





## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

---

Group, and CISA's Water and Wastewater Community of Interest group. Additionally, CISA's SED will continue to coordinate with other CISA Divisions to document an agency-wide requirement to develop and implement standard operations procedures to improve regular communication and information sharing related to the Water and Wastewater Systems Sector and other sectors, as appropriate.

CISA's efforts to address this recommendation, however, are dependent on the completion of updates to Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," currently dated February 12, 2013,<sup>4</sup> which is currently planned for no later than December 31, 2024. CISA expects that the updated PPD-21 will clarify SRMA roles and responsibilities and expectations for SRMA engagement with other Federal agencies. CISA will apply this guidance to determine appropriate roles for engagement with the EPA in its capacity as the SRMA for the Water and Wastewater Systems Sector, which will in turn determine how CISA Divisions will share and implement those roles. SED will establish this requirement as part of its FY 2025 Annual Operating Plan by October 31, 2024. Overall ECD: September 30, 2025.

---

<sup>4</sup> [https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508\\_0.pdf](https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf)



## OFFICE OF INSPECTOR GENERAL

*U.S. Department of Homeland Security*

### Appendix C: Sixteen Critical Infrastructure Sectors and Sector Risk Management Agencies

| Critical Infrastructure Sector         | Corresponding Sector Risk Management Agency |
|--|---|
| Chemical                               | DHS   |
| Commercial Facilities                  | DHS   |
| Communications                         | DHS   |
| Critical Manufacturing                 | DHS   |
| Dams                                   | DHS   |
| Defense Industrial Base                | DOD   |
| Emergency Services                     | DHS   |
| Energy                                 | DOE   |
| Financial Services                     | TREASURY                                    |
| Food And Agriculture                   | USDA & HHS                                  |
| Government Facilities                  | GSA & DHS                                   |
| Healthcare And Public Health           | HHS   |
| Information Technology                 | DHS   |
| Nuclear Reactors, Materials, And Waste | DHS   |
| Transportation Systems                 | DOT & DHS                                   |
| Water And Wastewater Systems           | EPA   |

Source: PPD-21



## **OFFICE OF INSPECTOR GENERAL**

*U.S. Department of Homeland Security*

---

### **Appendix D: Report Distribution**

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chiefs of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Under Secretary, Office of Strategy, Policy, and Plans  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees

## Additional Information

To view this and any other DHS OIG reports, Please visit our website: [www.oig.dhs.gov](http://www.oig.dhs.gov)

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)



## DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: [www.oig.dhs.gov/hotline](http://www.oig.dhs.gov/hotline)

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:  
Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive SW  
Washington, DC 20528-0305