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

January 9, 2024

MEMORANDUM FOR: Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.01.09 16:50:48 -07'00'

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

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.

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

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.

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.

Table of Contents

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

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.[1] Additionally, in March 2021, a former employee of a Kansas public water system was indicted for remotely accessing a protected computer without authorization.[2]

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).[3] 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),[4] 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.

---

[1] 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.

[2] 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.

[3] Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience | CISA.

[4] The *National Defense Authorization Act for FY 2021* redefined Sector-Specific Agencies as Sector Risk Management Agencies.

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.[5] 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.

---

[5] 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.

Table 1. CISA's Six Divisions and Key Functions

DIVISION	KEY FUNCTIONS
Cybersecurity Division*	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.
National Risk Management Center*	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.
Infrastructure Security Division*	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.
Integrated Operations Division*	Provides 24/7/365 situational awareness and near–real-time operational reporting; conducts all-source intelligence analysis and delivers cyber and physical vulnerability assessments.
Stakeholder Engagement Division*	Develops partnerships, facilitates dialogue, convenes stakeholders, and promotes awareness to help CISA achieve a secure and resilient infrastructure.
Emergency Communications Division	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
* 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.

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[6] 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.

---

[6] PPD-21 defines "collaboration" as the process of working together to achieve shared goals.

- <u>Web Application Scanning</u>: Non-intrusive checks of publicly accessible web applications to determine vulnerabilities, bugs, and weak configurations.

- <u>Cyber Resilience Review</u>: 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.

- <u>CISA Tabletop Exercise Packages</u>: 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*[7] (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.

---

[7] Public Law 115-278, (codified as 6 U.S.C. § 652(c)(6)).

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*[8] 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*[9] 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

---

[8] *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*, The White House, Office of the Press Secretary, February 12, 2013.
[9] 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*,[10] 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.

---

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

CISA Did Not Coordinate Effectively Between Divisions

According to the CISA Act,[11] 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.[12] 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

---

[11] Public Law 115-278, (codified as 6 U.S.C. § 652(c)(7)).

[12] *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.

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

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.

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.

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.

**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.

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.

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

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.[1] 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),[2] and clarified in Section 9002 of the National Defense Authorization Act for FY 2021.[3] 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

---

[1] https://www.cisa.gov/resources-tools/resources/cisas-free-cyber-vulnerability-scanning-water-utilities
[2] https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan
[3] Section 9002 of Pub Law No. 116-283, https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf

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

<u>OIG recommended that the CISA Director:</u>

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

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,[4] 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.

---

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

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

Appendix D:
Report Distribution

<u>Department of Homeland Security</u>

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

<u>Office of Management and Budget</u>

Chief, Homeland Security Branch
DHS OIG Budget Examiner

<u>Congress</u>

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: 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

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

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