ENERGY & COMMERCE
CHAIR RODGERS

MEMORANDUM January 29, 2024

TO: Members of the Subcommittee on Environment, Manufacturing, and Critical Materials

FROM: Committee Majority Staff

RE: Hearing entitled "Ensuring the Cybersecurity of America's Drinking Water Systems"

I. INTRODUCTION

The Subcommittee on Environment, Manufacturing, and Critical Materials has scheduled a hearing on Wednesday, January 31, 2024, at 2:00 p.m. (ET) in 2123 Rayburn House Office Building. The title of the hearing is "Ensuring the Cybersecurity of America's Drinking Water Systems." This hearing is a follow-up to the May 16, 2023, hearing held by the Subcommittee on Oversight and Investigations, entitled, "Protecting Critical Infrastructure from Cyberattacks: Examining Expertise of Sector Specific Agencies," at which the U.S. Environmental Protection Agency (EPA) testified. Witnesses are by invitation only.

II. WITNESSES

- **Cathy Tucker-Vogel**, Public Water Supply Section Chief, Kansas Department of Health and Environment *on behalf of the Association of State Drinking Water Administrators;*
- **Scott Dewhirst, P.E.**, Superintendent and Chief Operating Officer, Tacoma Water *on behalf of the Association of Metropolitan Water Agencies;*
- **Rick Jeffares**, President, Georgia Rural Water Association *on behalf of the National Rural Water Association;* and,
- **Kevin Morley, Ph.D.**, Manager-Federal Relations, American Water Works Association.

III. BACKGROUND

A. Evolving Cybersecurity Threats to Critical Infrastructure

Cyberattacks to critical infrastructure present a significant threat to the United States, affecting national security, the economy, and public health and safety.[1] The interconnected nature

[1] DEP'T OF HOMELAND SEC., Secure Cyberspace and Critical Infrastructure, https://www.dhs.gov/securecyberspace-and-critical-infrastructure (last visited May 10, 2023).

of critical infrastructure systems exposes them to attacks from foreign adversaries and criminals.[2] Recently, entities across multiple sectors have been attacked by an Iranian affiliate known as the CyberAv3ngers. The attacked entities include about a dozen water and wastewater systems, including the Municipal Water Authority of Aliquippa, Pennsylvania.[3] Cyberattacks against public water systems and all critical infrastructure are increasing.[4]

"Critical infrastructure" refers to "systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5] Because the operation and information systems of community water systems are electronic and computerized, these systems need to be mindful about their ability to defend their systems from cyberattacks.[6]

Moreover, drinking water systems play a crucial role in public health and the functioning of society (i.e., hospitals cannot perform surgeries; water pressure lessens in pipes, fomenting disease and preventing firefighting activities; and impacting electric utility and manufacturing operations[7]). For this reason, efforts within the drinking water sector have focused not just on prevention but also on "resilience"[8] — the capability to prepare for, withstand, recover from, and adapt to compromises of cyber resources.[9]

B. *Federal Cybersecurity Roles and Responsibilities*

Statutory directives on drinking water systems' security have existed in public law since 2002. However, in 2013, Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21) established a national policy on critical infrastructure security.[10] PPD-21 directed the Department of Homeland Security (DHS) to provide guidance and coordinate federal critical infrastructure resilience and security efforts, as well as identify critical infrastructure sectors and designate a Sector-Specific Agency (later renamed "Sector Risk Management Agencies" or SRMAs) for each sector.[11] SRMAs are supposed to collaborate with critical infrastructure owners and operators, carry out day-to-day coordination of sector-specific activities, execute incident management responsibilities, provide technical expertise and support for their sectors, and provide required information to DHS.[12] PPD-21 established the

[2] Id.
[3] https://www.usatoday.com/story/news/nation/2023/11/29/irans-cyber-av3ngers-target-israel-unitronics-devices-in-us/71741103007/
[4] https://www.epa.gov/waterresilience/epa-cybersecurity-water-sector
[5] Critical Infrastructures Protection Act of 2001, 4 U.S.C. 5195c(e); Critical Infrastructure Security and Resilience, Presidential Policy Directive-21, Feb 13, 2013 [hereinafter PPD-21]. The Water and Wastewater sector is considered "critical infrastructure" under PPD-21 and EPA is the Sector Risk Management Agency responsible for it.
[6] This is the definition of cybersecurity. https://csrc nist.gov/glossary/term/cyber_security
[7] https://www.domesticpreparedness.com/articles/water-and-wastewater-sector-perspectives
[8] 15 Cybersecurity Fundamentals for Water and Wastewater Utilities | WaterISAC
[9] https://csrc nist.gov/glossary/term/designing_for_cyber_resiliency_and_survivability
[10] Op. Cit.
[11] Op. Cit., William M. Thornberry National Defense Authorization Act for Fiscal Year 2021 § 9002(c)(3) (applying the term "Sector Risk Management Agency").
[12] Op. Cit.

Environmental Protection Agency (EPA) as the SRMA for the Water and Wastewater Systems Sector, which includes drinking water and wastewater utilities. Thus, the EPA and DHS must coordinate to utilize EPA expertise and assist critical infrastructure owners and operators in the Water and Wastewater Systems Sector. [13]

In addition, the EPA's Office of Water and Office of Homeland Security administer its water security programs and are responsible for overseeing implementation and enforcement of section 1433 of the Safe Drinking Water Act (SDWA).[14] The EPA also works jointly with the Department of Energy in operation of the Water Security Test Bed (WSTB) at the Idaho National Laboratory to focus on improving America's ability to safeguard water systems, respond to contamination incidents, and design better, more resilient infrastructure.[15] Research at the WSTB can also support cybersecurity defense and mitigation approaches for water infrastructure operational technology.[16]

C. Statutory Authorities Related to Cybersecurity and the Water Sector

Beginning in 2002, Congress[17] mandated that community water systems conduct vulnerability assessments of, and prepare emergency response plans for, their facilities (including "electronic, computer, or other automated systems") to "terrorist attacks or other intentional acts" that are "probable threats to…substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water."[18] Congress amended this mandate in 2018[19] to include risk and resilience assessments for these facilities, explicitly requiring a facility's emergency response plan to address identified vulnerabilities in systems' physical and cybersecurity.[20]

The 2018 amendment authorized technical assistance and grants to assist community water systems in addressing vulnerabilities and promoting outreach to the smallest water systems.[21] In addition to these requirements, the EPA maintains the ability to inspect facilities under SDWA section 1445 and issue penalties under SDWA section 1414. SDWA does not give the EPA regulatory authority related to cybersecurity.

The EPA does provide cybersecurity-related technical assistance to water systems and states.[22] SDWA Section 1442(b) authorizes the EPA to provide technical assistance and grants to states or publicly owned public water systems in emergency situations (including cybersecurity emergencies) in which the EPA determines there is a substantial danger to public health. It also

[13] See ENVTL. PROT. AGENCY & DEP'T OF HOMELAND SECURITY, Waste and Wastewater Sector-Specific Plan i (2015), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf.
[14] 42 U.S.C. § 300i-2.
[15] https://inl.gov/integrated-energy/idaho-test-bed-focuses-on-municipal-water-security/
[16] https://cfpub.epa.gov/si/si_public_file_download.cfm?p_download_id=531521
[17] Public Health Security and Bioterrorism Preparedness and Response Act, tit. IV, Pub. L. No. 107-188.
[18] Id. §401.
[19] America's Water Infrastructure Act of 2018 § 2013, Pub L. No. 115-270.
[20] Id. § 2013(b).
[21] SDWA §1433(g).
[22] See ENVTL. PROT. AGENCY, EPA Cybersecurity for the Water Sector, https://www.epa.gov/waterriskassessment/epa-cybersecurity-water-sector#TA

reauthorizes appropriations through fiscal year (FY) 2026 ($35 million/year for emergency Technical Assistance grants).

SDWA Section 1459F authorizes the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability program to assist public water systems (serving >10,000) in increasing drinking water system resilience, including cybersecurity. The statute lists 9 types of eligible projects, including projects to reduce cybersecurity vulnerabilities. The EPA received a $5,000,000 appropriation in FY2023 for this grant program.

SDWA Section 1459G mandates (subject to the availability of appropriations) a study that examines the state of current and potential future technology (including cybersecurity technology) for enhancing drinking water treatment, monitoring, affordability, or efficiency. It also authorizes a new EPA-managed competitive advanced drinking water technology grant program supporting the deployment of emerging technologies (including cybersecurity). It authorizes $10 million/year for the program through FY2026; the EPA has never received appropriations under this authority.

SDWA Section 1420A mandates that the EPA, in coordination with DHS, develop a prioritization framework to identify public water systems that, if impacted by a cybersecurity incident, would lead to significant impacts on public health and safety. The statute also requires the EPA, in coordination with DHS, to develop a voluntary Technical Cybersecurity Support Plan for public water systems that prioritizes systems for support, sets timelines, and identifies specific voluntary capabilities the EPA or DHS will offer. The EPA submitted these reports in FY2022.[23]

SDWA section 1452 contains authority for capitalization grants for State Revolving Loan Funds (SRFs). The EPA's March 2022 SRF Implementation Memorandum included guidance to states to utilize the significant SRF funding increase in the Infrastructure Investment and Jobs Act (IIJA) for infrastructure projects that make water systems more resilient to all threats—including new and emerging threats like cyber-attacks.

D. Additional Federal Funding Sources

There are several additional funding resources available to support drinking water and wastewater systems in implementing cyber projects. These include:

- Clean Water State Revolving Fund (CWSRF): Aids any public, private, or nonprofit entity for measures to increase the security of publicly owned treatment works, including cybersecurity.

- DHS State and Local Cybersecurity Grant Program (SLCGP): Provides for cybersecurity grants from state administrative agencies for states, cities, counties, and towns. Sub-award applications for cities, counties and towns must be submitted to the respective state administrative agency.

[23] Technical Cybersecurity Support Plan for Public Water Systems - Report to Congress (epa.gov)

• Tribal Cybersecurity Grant Program at DHS: Provides for grants to tribal governments to address (1) cybersecurity risks and (2) threats to their information systems.

E. Sector Directed Information Sharing

The Water and Wastewater Systems sector has both a Sector Coordinating Council (SCC) and a related Government Coordinating Council (GCC).[24] The SCCs are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities. The Water and Wastewater Systems SCC is supposed to serve as the sector's voice and coordinate and collaborate with sector-specific agencies (SSAs) and the Water and Wastewater Systems GCC to address the entire range of critical infrastructure security and resilience policies and efforts.[25] In addition, the SCCs are encouraged to establish voluntary practices to ensure that sector perspectives are included.[26]

In addition, the Water Information Sharing and Analysis Center (WaterISAC) is the designated information sharing and operations arm of the Water Sector Coordinating Council.[27] Established in 2002,[28] WaterISAC is a non-profit organization, comprised of water and wastewater utility managers and state drinking water administrators, and the only all-threats security information source for the water and wastewater sector.[29] WaterISAC is a single point source for data, facts, case studies, and analysis on water security and threats from intentional contamination, terrorism and cyber-crime.[30] WaterISAC also provides analysis and resources to support response, mitigation, and resilience initiatives.[31]

On January 9, 2024, the DHS Office of Inspector General (OIG) issued a Final Report covering FY 2019-2022 that found Cybersecurity and Infrastructure Security Agency (CISA) had extensive products and services available to its stakeholders to manage risks and mitigate cybersecurity threats to critical water and wastewater infrastructure.[32] However, CISA did not consistently collaborate with the EPA and the water sector to leverage and integrate its cybersecurity expertise with stakeholders' water expertise. According to the report, this occurred because CISA did not have a written agreement with the EPA regarding its interagency collaboration, nor policies or procedures to ensure appropriate collaboration with the EPA and other stakeholders.

[24] https://www.cisa.gov/water-sector-council-charters-and-membership

[25] https://www.cisa.gov/resources-tools/groups/sector-coordinating-councils

[26] Id.

[27] Id.

[28] https://www.waterisac.org/about-us, It was later authorized by Congress in the Public Health Security and Bioterrorism Preparedness and Response Act Bioterrorism Act of 2002.

[29] https://www.waterisac.org/about-us

[30] Id.

[31] Id.

[32] Cuffari, Joseph V. *CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Water and Wastewater Sector*, U.S. Department of Homeland Security Office of Inspector General, 9 Jan. 2024, www.oig.dhs.gov/sites/default/files/assets/2024-01/OIG-24-11-Jan24.pdf.

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 the OIG's 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.[33]

On January 18, 2024, CISA, FBI, and the EPA published an Incident Response Guide for the water sector. The purpose of the Incident Response Guide is to provide water sector owners and operators information about the federal roles, resources, and responsibilities for each stage of the cyber incident response lifecycle. The lifecycle can be broken down into four components: preparation, detection and analysis, containment eradication and recovery, and post-incident activity. Familiarity with Incident Response Guide information is intended to improve the water sector's ability to respond to—and recover from—a cyber incident.[34]

IV. DISCUSSION

Testimony and discussion are expected to address the following questions:

- What outreach does EPA engage in to carry out its responsibility as SRMA and where does the sector realize the greatest value from EPA?
- How does the sector incorporate its specialized knowledge to strengthen cybersecurity efforts?
- What are some of the emerging cybersecurity threats to critical infrastructure of which Congress should be aware?
- What is working well under current law and what still needs to be done to address future cybersecurity risks?

V. STAFF CONTACT

For questions regarding this hearing, please contact Mary Martin, Jerry Couri, or Drew Lingle of the Committee staff at (202) 225-3641.

[33] CISA Needs to Improve Collaboration to Enhance Cyber Resiliency in the Waste and Wastewater Sector (dhs.gov)
[34] Incident Response Guide: Water and Wastewater Sector (cisa.gov)