United States Senate

WASHINGTON, DC 20510

April 5, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Michael Regan
Administrator
Environmental Protection Agency

Dear Administrator Regan:

Critical infrastructure is comprised of "systems and 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."[1] Cyberattacks targeting our critical infrastructure sectors, which include energy, finance, food and agriculture, healthcare, municipal services, transportation, water, and others, put our national security at risk.[2]

As you are aware, the Environmental Protection Agency (EPA) is designated as a Sector Risk Management Agency (SRMA) for purposes of providing institutional knowledge and sector expertise for one of the sixteen Critical Infrastructure Sectors identified by the Cyber Security and Infrastructure Security Agency (CISA), namely, the water and wastewater sector.[3]

In November 2023, water systems in Texas and Pennsylvania were the victims of cyberattacks perpetrated by the groups Cyber Av3ngers and Daixin Team.[4] In Texas, Daixin Team managed to disrupt the business operations of the North Texas Municipal Water District.[5] In Pennsylvania, the Iranian-backed cybercriminal group Cyber Av3engers gained access to the systems managing water pressure at the Municipal Water Authority of Aliquippa, which resulted in the utility company replacing the affected equipment.[6] According to David Travers, the Director of the EPA's Water Infrastructure and Cyber Resilience Division, the lack of adoption of even simple cyber measures like multifactor authentication is the "most significant cyber risk

[1] 42 U.S.C. § 5195c(e).

[2] CISA, *Critical Infrastructure Sectors*, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors; *See also,* Stephen Webber, *Threats to America's Critical Infrastructure are now a Terrifying Reality*, The Hill (Feb. 11, 2024, 1:00 PM), https://thehill.com/opinion/technology/4458692-threats-to-americas-critical-infrastructure-are-now-a-terrifying-reality/.

[3] *Id*. at *Critical Infrastructure Sectors*, Water and Wastewater Systems.

[4] Chris Teale, *Two Recent Cyberattacks on Water Systems Highlight Vulnerability of Critical Infrastructure*, Route Fifty (Dec. 5, 2023), https://www.route-fifty.com/cybersecurity/2023/12/two-recent-cyberattacks-water-systems-highlight-vulnerability-critical-infrastructure/392500/.

[5] *Id*.

[6] *Id*.

in this sector. Consequently, many water and wastewater systems remain highly susceptible to cyberattacks that could disrupt their operations."[7]

A July 25, 2019, Government Accountability Office (GAO) report reviewed 23 federal agencies to assess their cybersecurity risk management programs.[8] The report found that "although the 23 agencies GAO reviewed almost always designated a risk executive, they often did not fully incorporate other key practices in their programs."[9] Specifically, the report noted that "until they address these practices, agencies will face an increased risk of cyber-based incidents that threaten national security and personal privacy."[10]

The GAO report made four recommendations to the EPA related to cybersecurity risk management strategies.[11] As of April 5, 2024, two of the recommendations remain open, one of which is a priority recommendation.[12] GAO's first open recommendation focuses on the need for the EPA to "establish a process for conducting an organization-wide cybersecurity risk assessment."[13] The second open recommendation tasks EPA, with "establishing and documenting a process for coordination between cybersecurity risk management and enterprise risk management functions."[14]

It is imperative that EPA continue to review and develop plans to protect the critical infrastructure it oversees. Additionally, it is vitally important that federal agencies and departments be in communication with each other as well as with private partners to ensure U.S. cybersecurity defense remains a priority.

Accordingly, please answer the following questions no later than April 19, 2024:

1. What steps has EPA taken to close each open recommendation from GAO's July 25, 2019, report? Provide all records.[15]

2. What does EPA consider to be the number one priority in the cybersecurity of the critical infrastructure it oversees? How does EPA prioritize cybersecurity threats to the critical infrastructure it oversees? Provide all records.

[7] *Id.*
[8] GAO, GAO-19-384, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (July 25, 2019), https://www.gao.gov/assets/d19384.pdf, EPA did not provide comments about whether or not it concurred with GAO's recommendations; see *also* https://www.gao.gov/products/gao-19-384 (Updates as to the status of the GAO recommendations).
[9] *Id.*
[10] *Id.*
[11] *Id.* at 70.
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] "Records" include any written, recorded, or graphic material of any kind, including letters, memoranda, reports, notes, electronic data (emails, email attachments, and any other electronically created or stored information), calendar entries, inter-office communications, meeting minutes, phone/voice mail or recordings/records of verbal communications, and drafts (whether they resulted in final documents).

3. What communications has EPA had with DHS, or other agencies, regarding cybersecurity initiatives for water and wastewater systems? Provide all records.

4. What is EPA's process for engaging private stakeholders in developing cybersecurity initiatives to protect critical infrastructure? Provide all records.

5. What exercises has EPA conducted, or does it plan on conducting, to test current programs in place for critical infrastructure cybersecurity defense? Provide all records.

6. What is EPA's process for reporting cybersecurity threats and attacks to federal agencies, Congress, and private stakeholders with respect to the critical infrastructure it oversees? Provide all records.

7. What is EPA's process to report and respond to cybersecurity attacks in real time? Provide all records.

8. How many cyberattacks have occurred on the critical infrastructure EPA oversees? What critical infrastructure was affected? Provide all records.

9. What kind and how many legacy IT systems has EPA identified in the water and wastewater systems sector? What are EPA's responsibilities to assist stakeholders in the protection and modernization of legacy IT systems? Provide all records.

In keeping with Executive Order 13526, please segregate all unclassified materials within the classified documents, and provide all unclassified information directly to the committee, and provide a classified addendum to the Office of Senate Security. Although the committee complies with all laws and regulations governing the handling of classified information, it is not bound, absent its prior agreement, by any handling restrictions.

Thank you for your prompt review and responses. If you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-0642.

Sincerely,

Chuck Grassley

Charles E. Grassley
Ranking Member
Committee on the Budget