United States Senate
WASHINGTON, DC 20510

April 5, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Jennifer E. Granholm
Secretary
Department of Energy

Dear Secretary Granholm:

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]

A January 30, 2024, Government Accountability Office (GAO) report selected four critical infrastructure sectors and relevant federal agencies responsible for oversight and support against ransomware attacks. The GAO report found ransomware attacks were one of the largest growing threats to national security.[3] Specifically, the report noted that ransomware became the fourth most reported cybersecurity incident in 2022 and accounted for 15% of financial losses from cybersecurity attacks that same year.[4] GAO also found the majority of policies in place to facilitate reporting of these ransomware attacks are "voluntary," and the government's priority is to "obtain technical details… rather than collect information about impacts."[5]

The GAO report made two recommendations to the Department of Energy (DOE) related to ransomware attack risk.[6] DOE did not concur with GAO's first recommendation, but did concur with the second recommendation.[7] GAO's first open recommendation focuses on the need for DOE, in coordination with Cybersecurity & Infrastructure Security Agency (CISA) and sector entities, to determine the extent to which the energy sector is adopting leading

[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] GAO, GAO-24-106220, *Critical Infrastructure Protection: Agencies Need to Enhance Oversight of Ransomware Practices and Assess Federal Support* (Jan. 30, 2024), https://www.gao.gov/assets/d24106221.pdf.
[4] *Id*. at 2.
[5] *Id*. at 27.
[6] *Id*. at 40-41.
[7] *Id.* at 60-61.

cybersecurity practices to reduce ransomware attacks.[8] The second open recommendation is that DOE, in coordination with CISA and other sector entities, should develop and implement routine evaluation procedures to measure how effective federal support is in assisting the energy sector reduce the risk of ransomware.[9]

It is imperative that DOE 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 DOE taken to close each open recommendation from GAO's January 30, 2024, report? Provide all records. [10]

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

3. What communications has DOE had with DHS, or other agencies, regarding cybersecurity initiatives for the energy sector? Provide all records.

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

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

6. What is DOE'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 DOE'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 DOE oversees? What critical infrastructure was affected? Provide all records.

---

[8] *Id*. at 40-41.
[9] *Id*.
[10] "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).

9. What kind and how many legacy IT systems has DOE identified in the energy sector? What are DOE'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,

Charles E. Grassley
Ranking Member
Committee on the Budget