United States Senate
WASHINGTON, DC 20510

April 5, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Janet Yellen
Secretary
Department of the Treasury

Dear Secretary Yellen:

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 Department of the Treasury (Treasury) 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 financial services sector.[3]

A September 17, 2020, Government Accountability Office (GAO) report reviewed the Treasury Department's ability to track the cybersecurity risk mitigation efforts of the financial services sector.[4] The report found that "[s]everal industry groups and firms are taking steps to enhance the security and resilience of the U.S. financial services sector through a broad range of cyber risk mitigation efforts."[5] However, the report noted that "Treasury does not track efforts or prioritize them according to goals established by the sector for enhancing cybersecurity and resiliency."[6]

---

[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*, Financial Services Sector.
[4] GAO, GAO-20-631, *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts* (Sept. 17, 2020), https://www.gao.gov/assets/gao-20-631.pdf; *See also* https://www.gao.gov/products/gao-20-631 (Updates as to the status of the GAO recommendations).
[5] *Id*.
[6] *Id*.

The GAO report made two priority recommendations to Treasury related to cybersecurity risk management strategies.[7] According to GAO, as of April 5, 2024, both of the priority recommendations remain open.[8] GAO's first open priority recommendation focuses on the need for Treasury to "coordinat[e] with the Department of Homeland Security [DHS] and other federal and nonfederal sector partners, track the content and progress of sectorwide cyber risk mitigation efforts, and prioritize their completion according to sector goals and priorities in the sector-specific plan."[9] The second open priority recommendation tasks Treasury to, in part, "update the financial services sector-specific plan to include specific metrics for measuring the progress of risk mitigation efforts and information on how the sector's ongoing and planned risk mitigation efforts will meet sector goals and requirements…."[10]

It is imperative that Treasury 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 Treasury taken to close each open priority recommendation from GAO's September 17, 2020, report? Provide all records.[11]

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

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

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

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

---

[7] *Id*. at 33.
[8] *Supra* note 4 (Updates as to the status of the GAO recommendations).
[9] *Id*. According to GAO, "[a]s of May 2023, Treasury said it is planning implementation of a tool that may enable it to track and record risks and resulting efforts, but that the tool's capabilities and uses were still in development."
[10] *Id*. According to GAO, "we reported in February 2023 that there was no deadline for the National Plan to be updated. As of May 2023, Treasury officials said they do not see a benefit in updating their sector specific plan in the interim."
[11] "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).

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

9. What kind and how many legacy IT systems has Treasury identified in the financial services sector? What are Treasury'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