United States Senate
WASHINGTON, DC 20510

April 5, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Lloyd J. Austin III
Secretary
Department of Defense

Dear Secretary Austin:

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 Defense (DOD) 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 defense industrial base sector.[3]

A November 14, 2022, Government Accountability Office (GAO) report reviewed the DOD's ability to manage and report cybersecurity incidents affecting the defense industrial base sector.[4] The report noted that "our nation's defense industrial base (DIB)—which includes entities outside the federal government that provide goods or services critical to meeting U.S. military requirements—[is] dependent on information systems to carry out their operations. These systems continue to be the target of cyberattacks, as DOD has experienced over 12,000 cyber incidents since 2015."[5]

The report found that "DOD's system for reporting all incidents often contained incomplete information and DOD could not always demonstrate that they had notified

[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*, Defense Industrial Base.
[4] GAO, GAO-23-105084, *DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared* (Nov. 14, 2022), https://www.gao.gov/assets/gao-23-105084.pdf; *see also* https://www.gao.gov/products/gao-23-105084 (Updates as to the status of the GAO recommendations).
[5] *Id*.

appropriate leadership of relevant critical incidents."[6] Specifically, the report noted, "[t]he weaknesses in the implementation of the two processes are due to DOD not assigning an organization responsible for ensuring proper incident reporting and compliance with guidance."[7] Additionally, the report notes that "DOD has not yet decided whether DIB cyber incidents detected by cybersecurity service providers should be shared with all relevant stakeholders."[8] Finally, the report states that DOD has established a policy for informing victims of a breach of their personally identifiable information; however, "DOD has not consistently documented the notifications of affected individuals, because officials said notifications are often made verbally or by email and no record is retained."[9]

The GAO report made six recommendations, which DOD concurred with, related to DOD's cyber incident reporting.[10] According to GAO, as of April 5, 2024, all six recommendations remain open.[11]

It is imperative that DOD 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 DOD taken to close each open priority recommendation from GAO's November 14, 2022, report? Provide all records.[12]

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.* at 36. (Recommendation 1) The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN assign responsibility for overseeing cyber incident reporting and leadership notification, and ensuring policy compliance; (Recommendation 2) The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN align policy and system requirements to enable DOD to have enterprise-wide visibility of cyber incident reporting to support tactical, strategic, and military strategies for response; (Recommendation 3) The Secretary of Defense should ensure that the DOD CIO, Commander of CYBERCOM, and Commander of JFHQ-DODIN include in new guidance on incident reporting include detailed procedures for identifying, reporting, and notifying leadership of critical cyber incidents; (Recommendation 4) The Secretary of Defense should ensure that the Commander of CYBERCOM—in coordination with DOD CIO and Directors of DC3 and DCSA—examines whether information on DIB-related cyber incidents handled by CSSPs is relevant to the missions of other DOD components, including DC3 and DCSA, and identifies when and with whom such information should be shared; (Recommendation 5) The Secretary of Defense should ensure that the DOD CIO determines what actions need to be taken to encourage more complete and timely mandatory cyber incident reporting from DIB companies; (Recommendation 6) The Secretary of Defense should ensure—through the Director of the Privacy, Civil Liberties, and Freedom of Information Directorate—that DOD components document instances where individuals affected by a privacy data breach were notified.
[11] *Supra* note 4 (Updates as to the status of the GAO recommendations).
[12] "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).

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

3. What communications has DOD had with DHS, or other agencies, regarding cybersecurity initiatives for the defense industrial base sector? Provide all records.

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

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

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

9. What kind and how many legacy IT systems has DOD identified in the Defense Industrial Base? What are DOD'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