United States Senate
WASHINGTON, DC 20510

July 3, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Dear Director Easterly:

According to the Cybersecurity and Infrastructure Security Agency (CISA), it was the victim of a cybersecurity intrusion from January 23-26, 2024.[1] Specifically, potential malicious activity affected CISA's Chemical Security Assessment Tool (CSAT) Ivanti Connect Secure appliance, resulting in "potential unauthorized access of Top-Screen surveys, Security Vulnerability Assessments, Site Security Plans, Personnel Surety Program (PSP) submissions, and CSAT user accounts."[2] Further, according to recent reports, CISA's Infrastructure Protection (IP) Gateway, now named CISA Gateway, was breached, potentially exposing critical information about the operations of our U.S. infrastructure.[3] These breaches of the agency tasked with the protection of our nation's cybersecurity and infrastructure security is cause for serious concern.

I've sounded the alarm about the critical need to improve the protection of our nation's cybersecurity.[4] Specifically, on March 4, 2024, I wrote you regarding the protection of critical infrastructure and CISA's prioritization of misinformation and disinformation over the protection of our nation's critical infrastructure. On April 29, 2024, CISA provided a response that failed to fully answer all the questions.[5] I also wrote letters to seven of the Sector Risk Management Agencies responsible for overseeing our nation's critical infrastructure to highlight the threat of ransomware attacks and other cyberattacks on our critical infrastructure sectors.[6] It appears

---

[1] CISA, *Chemical Security Assessment Tool (CSAT) Ivanti Notification*, https://www.cisa.gov/chemical-security-assessment-tool-csat-ivanti-notification.
[2] *Id.*
[3] Jonathan Greig and Suzanne Smalley, The Record, *CISA forced to take two systems offline last month after Ivanti compromise* (Mar. 8, 2024), https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise; *see also* Julie Pattison-Gordon, *Government Technology*, *Federal Cyber Agency Offlines 2 Systems After Ivanti Hack* (Mar. 13, 2024), https://www.govtech.com/security/federal-cyber-agency-offlines-2-systems-after-ivanti-hack.
[4] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity & Infrastructure Security Agency (Mar. 4, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_critical_infrastructure.pdf; *see also* Sen. Charles E. Grassley, *Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense* (Apr. 8, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-federal-agencies-must-stop-dragging-their-feet-on-bolstering-cybersecurity-defense.
[5] On File with Committee Staff.
[6] *Supra* note 4. *Grassley: Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense*.

CISA hasn't taken adequate steps to ensure the safety of its own systems, leaving the nation at risk.

Accordingly, so Congress may conduct objective and independent oversight concerning CISA's efforts to address these recent cyberattacks, please provide answers to the following no later than July 17, 2024:

1. Provide a full and complete list of all tools, gateways, databases, and systems that were breached, or potentially breached, as a result of the January 23-26 cyberattack.

2. Provide a full and complete list of all facilities, organizations, and individuals who were affected by the January 23-26 cyberattack. Has CISA notified these entities about the cyberattack and that their information could potentially be subject to misuse?

3. Did CISA know about the exploitation of Invanti vulnerabilities prior to the January 23-26 attack?[7] If so, what specific measures did CISA take to secure their tools, gateways, databases, and systems from these vulnerabilities? Provide all records.[8]

4. Did CISA conduct its own independent risk assessment of the Ivanti system prior to its use at CISA? If not, did CISA conduct that risk assessment before the cyberattack? Provide all records.

5. When exactly did CISA become aware of the cyberattack?

6. Please describe how CISA identified the cybersecurity intrusion. Provide all records.

7. How many records were accessible during the cyberattack? How many records were actually accessed? Provide all records.

8. What specific steps is CISA taking to ensure these types of attacks don't occur in the future? Provide all records.

9. Has CISA identified who or what entity or organization perpetrated the attacks? If so, who or what entity or organization was the orchestrator of the attack and what is being done about it?

---

[7] CISA, *CISA, U.S. and International Partners Warn of Ongoing Exploitation of Multiple Ivanti Vulnerabilities* (Feb. 29, 2024), https://www.cisa.gov/news-events/news/cisa-us-and-international-partners-warn-ongoing-exploitation-multiple-ivanti-vulnerabilities#:~:text=WASHINGTON%20%E2%80%93%20The%20Cybersecurity%20and%20Infrastructure%20Security%20Agency,Ivanti%20Connect%20Secure%20and%20Ivanti%20Policy%20Secure%20gateways.

[8] "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).

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