United States Senate

WASHINGTON, DC 20510

May 19, 2026

Mr. Nick Andersen
Acting Director
Cybersecurity and Infrastructure Security Agency, Stop 0380
U.S. Department of Homeland Security
245 Murray Lane
Washington, DC 20528

Dear Acting Director Andersen:

I write to request an urgent classified briefing regarding public reporting that a contractor for the Cybersecurity and Infrastructure Security Agency (CISA) maintained lists of agency accounts and passwords on a public database.[1] This reported incident raises serious questions about how such a security lapse could occur at the very agency charged with helping to prevent cyber breaches. According to a recent report from Krebs on Security, this leak included files that detailed how CISA builds, tests, and deploys software internally in a folder called "Private-CISA."[2] Exposed files reportedly included a file named "importantAWStokens," with the administrative credentials to three Amazon Web Services (AWS) servers, and one named "AWS-Workspace-Firefox-Passwords.csv," with plaintext usernames and passwords for multiple internal systems.[3] Security experts cited in recent reporting have described this security lapse as "one of the most egregious government data leaks in recent history."[4]

This reporting raises serious concerns regarding CISA's internal policies and procedures at a time of significant cybersecurity threats against U.S. critical infrastructure. For example, last month CISA released an advisory on threats to critical infrastructure from Iranian-affiliated cyber actors, which stated that these parties have disrupted computers used in manufacturing "across several U.S. critical infrastructure sectors…resulting in operational disruption and financial loss."[5] The alleged data leak has also occurred against the backdrop of major disruptions internally at CISA.[6] In 2025, for example, CISA lost more than a third of its

---

[1] Brian Krebs, *CISA Admin Leaked AWS GovCloud Keys on Github*, Krebs on Security (blog) (May 18, 2026) (krebsonsecurity.com/2026/05/cisa-admin-leaked-aws-govcloud-keys-on-github/).

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Cybersecurity and Infrastructure Security Agency, *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure* (AA26-097A) (Apr. 7, 2026).

[6] *Exclusive: One-Third of Top U.S. Cyber Force has Left Since Trump Took Office*, Axios (June 3, 2025) (www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts).

workforce, including almost all its senior leaders, raising questions in the private sector and Congress about the direction of the agency.[7]

CISA's public statement that "there is no indication that any sensitive data was compromised as a result of this incident" leaves unanswered questions about the policies and procedures that made it possible for this incident to reportedly occur in the first place. Given the potentially significant impact of this data leak, I request a briefing at the highest classification level necessary, as soon as possible, and no later than June 5, 2026, to discuss these matters in detail. The briefing should, at a minimum, address the following questions about the reported incident:

1. When did CISA first become aware of the exposure and how was it discovered?

2. What actions did CISA take immediately after discovering the exposure? How long did these actions take?

3. What specific systems, credentials, or other sensitive information were exposed in the public repositories, and what level of access did those credentials provide?

4. How long were the repositories and exposed credentials publicly accessible, and were the repositories accessed by unauthorized parties?

5. Did any unauthorized actor successfully use the exposed credentials or otherwise exploit the exposure to access CISA systems, networks, or data?

6. What forensic and incident-response actions did CISA undertake following discovery of the exposure? If these actions are ongoing, please describe the timeline for completion.

7. What contractor or subcontractor was responsible for the repositories and credentials, what contractual cybersecurity requirements applied, and were those requirements violated?

8. Why did existing CISA security controls fail to prevent or detect the exposure? Did CISA comply with applicable federal cybersecurity requirements, and if not, what specific control failures or deficiencies contributed to the incident?

[7] *Exclusive: One-Third of Top U.S. Cyber Force has Left Since Trump Took Office*, Axios (June 3, 2025) (www.axios.com/2025/06/03/cisa-staff-layoffs-resignations-trump-cuts); *IBM Executive Floated for CISA Director as Concerns Persist for Agency*, SC Media (May 18, 2026) (www.scworld.com/news/ibm-executive-floated-for-cisa-director-as-concerns-persist-for-agency); *DHS Nominee Mullin Pressed on Restoring CISA Staffing*, The Record (Mar. 18, 2026) (therecord.media/dhs-mullin-pressed-on-restoring-cisa-staffing).

9. To what extent does this incident reflect potential broader systemic weaknesses in CISA security practices, including the management of public code repositories?

10. What corrective actions has CISA implemented or planned to implement to ensure that similar exposures do not recur?

11. What standard process, if any, does CISA maintain for responding to external communications that raise awareness of security flaws?

12. What training, if any, do CISA employees who manage public facing communication accounts receive regarding passing on potentially actionable security information?

Thank you for your prompt attention to these matters. If you have any questions related to this request, please contact Nick Caron at Nick_Caron@hassan.senate.gov. Please send any official correspondence relating to this request to Nick_Caron@hassan.senate.gov.

Sincerely,

Margaret Wood Hassan
United States Senator