ANDREW R. GARBARINO, NEW YORK
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

May 19, 2026

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

Dear Acting Director Andersen:

We write to express our deep concern regarding reports that the Cybersecurity and Infrastructure Security Agency (CISA) left exposed on GitHub credentials to highly privileged AWS GovCloud accounts and several of CISA's internal systems.[1] We demand a briefing as soon as possible on how this serious security lapse occurred, any potential security consequences, remediation activities, corrective actions related to the contractor personnel involved, and efforts to monitor for and prevent similar activity from occurring in the future.

As you are likely aware, on May 18, 2025, reporting emerged that a security researcher scanning GitHub for exposed information identified a repository titled "Private-CISA," which was created in November 2025. The repository contained "a vast number of internal CISA/DHS credentials and files, including cloud keys, tokens, plaintext passwords, logs and other sensitive CISA assets."[2] One exposed file was titled "importantAWStokens." Another was titled "AWS-Workspace-Firefox-Passwords.csv," and contained usernames and passwords for internal CISA systems. We were disturbed to learn that the exposed AWS keys remained valid for 48 hours after CISA was notified of the "Private-CISA" repository on GitHub.[3]

The "Private-CISA" repository was reportedly managed by an employee working for a CISA contractor, Nightwing.[4] Troublingly, the researcher discovered that the CISA administrator had disabled GitHub's default settings intended to prevent the publishing of sensitive information on the platform.[5] We cannot fathom any compelling reason to disable these default settings.

It is no secret that our adversaries – like China, Russia, and Iran – seek to gain access to and persistence on Federal networks. The files contained in the "Private-CISA" repository provided

[1] Brian Krebs, *CISA Admin Leaked AWS GovCloud Keys on Github*, KREBSONSECURITY (May 19, 2026), https://krebsonsecurity.com/2026/05/cisa-admin-leaked-aws-govcloud-keys-on-github/.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *Id.*

the information, access, and roadmap to do just that. Security researchers said the content openly available online included information on "how CISA builds, tests and deploys software internally," and they described it as "one of the most egregious government data leaks in recent history."[6] We agree.

We are concerned that this incident reflects a diminished security culture and/or an inability for CISA to adequately manage its contract support. Over the past year, the Trump Administration has decimated CISA's workforce, and it lost nearly 1,000 personnel. Previous Department of Homeland Security (DHS) and CISA leadership unleashed special government employees from the Department of Government Efficiency (DOGE) on the Department and CISA.[7] It is unclear exactly what systems DOGE employees accessed, but we do know that they demonstrated gross disregard for basic security practices.[8] While we appreciate that you are working to expeditiously hire 300 people,[9] we worry that a substantially reduced workforce, coupled with the Administration's indifference to security, created the conditions that allowed such a significant security lapse to occur. Moreover, we are concerned that the incident undermines CISA's credibility.

We understand the past 18 months have been difficult for CISA and its employees, and we are committed to working with you to put it back on track to execute its Federal network security and critical infrastructure missions. However, we need assurances that CISA is taking this incident seriously, and that you will do everything in your power to fully assess the security consequences of this lapse and to prevent anything like it from happening again.

We look forward to scheduling a briefing from you on this incident as soon as possible and ensuring you have the personnel, resources, and authorities necessary to address the impacts of this serious lapse and prevent similar incidents in the future.

Sincerely.

Bennie G. Thompson
Ranking Member
Committee on Homeland Security

Delia C. Ramirez
Ranking Member
Subcommittee on Cybersecurity and Infrastructure Protection

Cc: The Hon. Andrew R. Garbarino, Chairman, Committee on Homeland Security
The Hon. Andy Ogles, Chairman, Subcommittee on Cybersecurity and Infrastructure Protection

[6] *Id.*
[7] Kim Zetter, *DOGE Now Has Access to the Top US Cybersecurity Agency*, WIRED (Feb. 19, 2025), https://www.wired.com/story/doge-cisa-coristine-cybersecurity/.
[8] *See e.g.* Makena Kelly & Vittoria Elliott, *DOGE Is Building a Master Database to Surveil and Track Immigrants*, WIRED (Apr. 18, 2025), https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/?_sp=97b5fec5-00ff-4064-a051-1332650e15ce.1779217521125; Brian Krebs, *DOGE to Fired CISA Staff: Email Us Your Personal Data*, KREBSONSECURITY (Mar. 19, 2025), https://krebsonsecurity.com/2025/03/doge-to-fired-cisa-staff-email-us-your-personal-data/.
[9] Justin Doubleday, *CISA Eyes Plan for More than 300 New Hires,* FEDERAL NEWS NETWORK (Mar. 25, 2026), https://federalnewsnetwork.com/cybersecurity/2026/03/cisa-eyes-plan-for-more-than-300-new-hires/.