United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

June 11, 2026

VIA ELECTRONIC TRANSMISSION

Mr. Nicholas M. Andersen
Acting Director
Cybersecurity and Infrastructure Security Agency

Dear Acting Director Andersen:

On May 18, 2026, it was reported that a contractor-employee for the Cybersecurity & Infrastructure Security Agency (CISA) maintained a public GitHub repository, a cloud-based platform used to store and share information for purposes of developing software code, that stored CISA credentials to several highly sensitive AWS GovCloud accounts and a large number of internal CISA systems, including passwords and cloud keys.[1] The title of the public repository was reportedly "Private-CISA."[2] Reports stated "a review of the GitHub account and its exposed passwords show the 'Private-CISA' repository was maintained by an employee of Nightwing."[3] It was also reported the GitHub account that included the repository titled "Private-CISA" was taken offline shortly after at least two cyber-security research companies notified CISA of the exposure, but the exposed AWS keys continued to remain valid for another 48 hours.[4]

CISA spokesperson Marco DiSandro said the agency is "aware of the reported exposure and is continuing to investigate the situation," and that there is "no indication that any sensitive data was compromised as a result of this incident."[5] However, according to reports, CISA would not say if the agency has seen any evidence of a breach stemming from this exposure.[6]

As you may be aware, I've previously raised concerns about the need to protect our nation's cybersecurity.[7] For instance, on April 8, 2024, I wrote letters to seven of the Sector

---

[1] Brian Krebs, *CISA Admin Leaked AWS GovCloud Keys on GitHub* (May 18, 2026), KREBSONSECURITY, https://krebsonsecurity.com/2026/05/cisa-admin-leaked-aws-govcloud-keys-on-github/; Zack Wittaker, *US cyber agency CISA exposed reams of passwords and cloud keys to the open web* (May 19, 2026), TECH CRUNCH, https://techcrunch.com/2026/05/19/us-cyber-agency-cisa-exposed-reams-of-passwords-and-cloud-keys-to-the-open-web/; Tim Starks, *CISA credential leak raises alarms, and Capitol Hill demands answers* (May 19, 2026), CYBERSCOOP, https://cyberscoop.com/cisa-credential-leak-congress-demands-answers/; Jessica Lyons, *America's top cyber-defense agency left a GitHub repo open with passwords, keys, tokens – and incredibly obvious filenames* (May 19, 2026), THE REGISTER, https://www.theregister.com/security/2026/05/19/americas-top-cyber-defense-agency-left-a-github-repo-open-with-with-passwords-keys-tokens-and-incredibly-obvious-filenames/5242915; *see also*, GitHub, *About GitHub and Git* (Last Viewed May 20, 2026), https://docs.github.com/en/get-started/start-your-journey/about-github-and-git#about-git.

[2] *Id.*

[3] Brian Krebs, *CISA Admin Leaked AWS GovCloud Keys on GitHub* (May 18, 2026), KREBSONSECUIRTY, https://krebsonsecurity.com/2026/05/cisa-admin-leaked-aws-govcloud-keys-on-github/.

[4] *Id.*

[5] Zack Wittaker, *US cyber agency CISA exposed reams of passwords and cloud keys to the open web* (May 19, 2026), TECH CRUNCH, https://techcrunch.com/2026/05/19/us-cyber-agency-cisa-exposed-reams-of-passwords-and-cloud-keys-to-the-open-web/.

[6] *Id*.

[7] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Alejandro Mayorkas, Secretary, Department of Homeland Security, the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency, and Mr. Ronald R. Rowe, Acting Director, United States Secret Service (Nov. 1, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Merrick Garland, Attorney General, Department of Justice, and the Honorable Christopher Wray, Director, Federal Bureau of Investigation (Nov. 1, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_doj_and_fbi_-_salt_typhoon_cyberattack.pdf; Press Release, Sen. Charles E.

Risk Management Agencies responsible for overseeing our nation's critical infrastructure to highlight the threat of cyberattacks on our critical infrastructure sectors.[8] I also wrote to CISA on July 3, 2024, and March 11, 2025, regarding a cyberattack, which released "critical information about the operation of U.S. infrastructure."[9] Most recently, on February 5, 2026, I wrote to CISA regarding allegations that CISA's previous acting director may have exposed sensitive CISA information on a public version of ChatGPT.[10]

Given that CISA is the agency charged with overseeing U.S. cybersecurity, it's imperative that CISA, and any contractor working on behalf of CISA, protects the agency's sensitive information. Accordingly, please respond to the following no later than June 25, 2026:

1. Is the reporting accurate? Did a public GitHub repository maintained by a government contractor expose credentials to AWS GovCloud Account and internal CISA systems along with information detailing how CISA builds, tests and deploys software internally? Was the repository maintained by an employee of Nightwing? Provide a timeline of when the repository was created, when CISA became aware, and when CISA took remedial steps to protect the information.

2. How long were the credentials to AWS GovCloud Account and internal CISA systems accessible on the public GitHub repository?

3. Has CISA revoked and replaced all exposed credentials? Once CISA was notified of the exposure, how long did it take for CISA to revoke and replace all credentials?

4. Have you evaluated if there was any sensitive data that was compromised as a result of this incident? If not, why not? Provide all records related to your incident response for this event.[11]

5. What CISA policies govern government contractors' use of external public versions of cloud-based platforms used to store and share information, such as GitHub? Please provide copies of these policies.

Grassley, *Grassley Conducts Sweeping Oversight of Recent AT&T Hack, Potential National Security Implications* (Aug. 5, 2024), https://www.grassley.senate.gov/news/news-releases/grassley-conducts-sweeping-oversight-of-recent-atandt-hack-potential-national-security-implications; Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (July 3, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; see also Press Release, 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.

[8] Press Release, 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.

[9] Letter from Sen. Charles E. Grassley, Ranking Member, Senate Budget Committee, to the Honorable Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency (July 3, 2024), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_cyberattack.pdf; Letter from Sen. Charles E. Grassley, Chairman, Senate Judiciary Committee, to Ms. Bridget Bean, Executive Director, Cybersecurity and Infrastructure Security Agency (Mar. 11, 2025), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_csat_hack_follow_up.pdf.

[10] Letter from Sen. Charles E. Grassley, Chairman, Senate Judiciary Committee to the Honorable Madhu Gottumukkala, Acting Director, Cybersecurity and Infrastructure Security Agency (Feb. 5, 2026), https://www.grassley.senate.gov/imo/media/doc/grassley_to_cisa_-_chatgpt.pdf.

[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 after action analysis and mitigation strategies have been conducted and implemented to make sure an incident like this does not happen again?

Thank you for your prompt attention to this matter. Should you have any questions, please contact Tucker Akin on my Committee staff at (202) 224-5225.

Sincerely,

Charles E. Grassley
Chairman
Committee on the Judiciary