MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

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

March 26, 2025

The Honorable Kristi Noem
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Noem:

We write to express our grave concerns regarding the revelation that top officials in the Trump administration use Signal, a commercial open-source messaging application, to discuss sensitive and possibly classified information and to inquire whether you participate in Signal discussions related to official government business.

As you are likely aware, a story appeared in *The Atlantic* titled "The Trump Administration Accidentally Texted Me Its War Plans."[1] Editor-in-chief Jeffrey Goldberg revealed that he had been inadvertently added to a Signal chat group called "Houthi PC small group." Over 48 hours, Mr. Goldberg observed a cavalier conversation about military operations against the Houthis in Yemen unfold in the chat.

Unfortunately, the indiscretion of the Vice President, the Director of National Intelligence, National Security Advisor, the Secretary of Defense, the Secretary of State, the White House Chief of Staff, the White House Deputy Chief of Staff for Policy, and other top Trump advisors was on full display in the Signal chat. Despite apparently detailed discussion of military operations, no one appeared to have objected to the conversation taking place on Signal. That leaves the impression that discussions about sensitive national security matters on Signal are common occurrences for the Trump administration. Given your vital role in national security matters, it stands to reason that you may have participated in such exchanges.

As the Secretary of the Department of Homeland Security (DHS or the Department) that houses the Cybersecurity and Infrastructure Security Agency (CISA), we assume you know of ongoing efforts by foreign adversaries to gain access to sensitive communications of government officials. State-sponsored threat actors from China have persistently sought access to government information, most recently by hacking into our top telecommunications companies and gaining access to the communications and data on the phones of then-President-elect Trump and then-

[1] Jeffrey Goldberg, *The Trump Administration Accidentally Texted Me Its War Plans,* THE ATLANTIC (Mar. 24, 2025), https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/.

Vice President-elect Vance.[2] The Russian government, for example, has sought to gain access to government information systems through sophisticated supply chain campaigns,[3] gaining access to networks of trusted government vendors,[4] and targeted spear-phishing.[5] Indeed, just last month, reports emerged that the Russian hackers sought to exploit Signal's linked devices capability to gain access to encrypted chats.[6] In light of these, and many, many other threats to the security of government information, the Federal Government has over time put in place a series of laws and policies designed to keep sensitive information out of the wrong hands while honoring the obligations of a free and open government by preserving government records.

We trust that you have been informed of your obligations under the Espionage Act,[7] Executive Order 13526 – *Classified National Security Information*,[8] Federal policies governing the handling of classified and sensitive information, and the Federal Records Act.[9] We expect that you have advised your staff of their responsibilities under Federal laws and policies governing the handling of information related to national security and official government business. We similarly trust that you and your staff are aware of the obligations of your White House colleagues under the Presidential Records Act.[10] Unfortunately, Monday's reporting in *The Atlantic* calls into question the diligence of the Trump administration's compliance with Federal laws and policies related to the handling of sensitive government information.

The public deserves to be confident that the government's highest-ranking officials are not sacrificing security for convenience by having conversations on Signal that should be happening in a sensitive compartmented information facility (SCIF). And our democracy demands that Federal and Presidential records are appropriately preserved. Accordingly, we ask that you respond to the following questions by April 2, 2025.

1. Are you complying with your obligations under the Espionage Act,[11] Executive Order 13526,[12] Federal policies governing the handling of classified and sensitive information, and the Federal Records Act?[13]

---

[2] Derek B. Johnson, *CISA Director Says Threat hunters Spotted Salt Typhoon on Federal Networks Before Telco Companies*, CYBERSCOOP (Jan. 15, 2025), https://cyberscoop.com/salt-typhoon-us-government-jen-easterly-cisa/.
[3] *See* U.S. Gov't Accountability Off., SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Apr. 22, 2021), https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.
[4] *See* Rebecca Heilweil, et al., *Federal Government Affected by Russian Breach of Microsoft*, CYBERSCOOP (Apr. 4. 2025), https://cyberscoop.com/federal-government-russian-breach-microsoft/.
[5] *See* Maya Mehrara, *Russian Hackers Targeting U.S. Official Ahead of Election, Microsoft Warns,* NEWSWEEK (Nov. 5, 2024), https://www.newsweek.com/russian-hackers-targeting-us-officials-ahead-election-microsoft-warns-1977178.
[6] Ryan Naraine, *How Russian Hackers Are Exploiting Signal 'Linked Devices' Feature for Real-Time Spying*, SECURITYWEEK (Feb. 19, 2025), https://www.securityweek.com/how-russian-hackers-are-exploiting-signals-linked-devices-for-real-time-spying/.
[7] 18 U.S.C. § 793.
[8] Exec. Order No. 13526, 75 Fed. Reg. 1013 (Jan. 8, 2010).
[9] 44 U.S.C. Chapters 21, 29, 31, and 33.
[10] 44 U.S.C. §§2201-09.
[11] 18 U.S.C. § 793.
[12] Exec. Order No. 13526, 75 Fed. Reg. 1013 (Jan. 8, 2010).
[13] 44 U.S.C. Chapters 21, 29, 31, and 33.

2. Have you ensured that all new political appointees at the Department have been advised of their obligations under the Espionage Act,[14] Executive Order 13526,[15] Federal policies governing the handling of classified and sensitive information, and the Federal Records Act?[16] Please describe the process through which such appointees were advised of their obligations under each law and policy and any additional training they have received.

3. Do you engage in discussions about official business via Signal or any other commercial messaging application?
    a. If you engage in discussions about official business on a commercial messaging application that is not Signal, please provide the name of the application.
    b. With whom do you engage in discussions about official business on Signal or other commercial messaging applications?
    c. If you engage in discussions about official business on a commercial messaging application, what is the process for maintaining records pursuant to the Federal Records Act?
    d. Please provide the Committee a copy of all communications you have engaged in regarding official government business via Signal or any other commercial messaging application.

4. Has DHS approved the use of Signal or any other commercial messaging application for the discussion of official business?
    a. Which commercial messaging applications have been approved for the discussion of official business? On what date was each application approved?
    b. Please provide a copy of the policy governing approval of commercial messaging applications for official use.

5. Has DHS approved Signal or any other commercial messaging application for the discussion of classified information?
    a. Which commercial messaging applications have been approved for use for the discussion of classified information? On what date was each application approved?
    b. Please provide a copy of the policy governing approval of commercial messaging applications for the discussion of classified information.

We believe that DHS plays a central role in keeping Americans safe, our critical infrastructure secure, and our communities resilient. We hope that you share that view. We are sure you can appreciate the importance of adhering to laws and policies governing the handling of government information.[17] On the best day, the Department's 260,000 employees have a challenging job, which has been made harder in recent weeks as its workforce has been arbitrarily gutted.

[14] 18 U.S.C. § 793.
[15] Exec. Order No. 13526, 75 Fed. Reg. 1013 (Jan. 8, 2010).
[16] 44 U.S.C. Chapters 21, 29, 31, and 33.
[17] *See* Devlin Barrett, *F.B.I. Calls D.H.S. Secretary's Criticism 'Deeply Irresponsible,'* N.Y. Times (Feb. 14, 2025) (quoting Secretary Noem, "The F.B.I. is so corrupt. We will work with any and every agency to stop leaks and prosecute these crooked deep state agents to the fullest extent of the law."), https://www.nytimes.com/2025/02/14/us/politics/fbi-kristi-noem-dhs.html.

Revealing sensitive operational information on sloppy text chains would only exacerbate the challenges DHS employees already experience carrying out their mission.

We look forward to your prompt response.

Sincerely,

Bennie G. Thompson
Ranking Member

Eric Swalwell
Member of Congress

J. Luis Correa
Member of Congress

Shri Thanedar
Member of Congress

Seth Magaziner
Member of Congress

Dan Goldman
Member of Congress

Delia C. Ramirez
Member of Congress

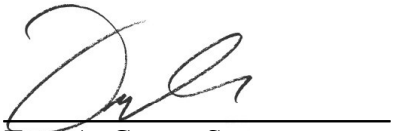
Timothy M. Kennedy
Member of Congress

LaMonica McIver
Member of Congress

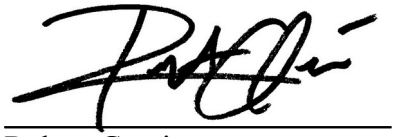
Julie Johnson
Member of Congress

Pablo José Hernández
Member of Congress

Nellie Pou
Member of Congress



Troy A. Carter, Sr.
Member of Congress



Robert Garcia
Member of Congress