

United States Senate
WASHINGTON, DC 20510

November 1, 2024

VIA ELECTRONIC TRANSMISSION

The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency

Mr. Ronald L. Rowe, Jr.
Acting Director
United States Secret Service

Dear Secretary Mayorkas, Director Easterly, and Acting Director Rowe:

On October 25, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) announced that the agencies are investigating the “unauthorized access to commercial telecommunications infrastructure” by actors affiliated with China.¹ This attack was reportedly a months-long espionage operation led by hackers from a group called “Salt Typhoon” and targeted data from the phones of former President Trump, vice presidential candidate and Senator J.D. Vance, and members of the Harris campaign.² Allegedly, the group was able to collect audio from phone calls and unencrypted communications including text messages.³ It’s also reported that Salt Typhoon conducted another cyberattack this month targeting major telecom providers including AT&T and Verizon and the system the federal government uses for court-authorized network wiretapping requests.⁴ These breaches potentially exposed millions of Americans’ internet data and sensitive government information to China.⁵

I’ve previously raised concerns about the need to protect our nation’s cybersecurity and U.S. critical infrastructure from national security threats.⁶ I wrote to 17 federal agencies on August 2, 2024,

¹ Press Release, FBI, *Joint Statement by FBI and CISA on People’s Republic of China Activity Targeting Telecommunications* (Oct. 25, 2024), https://www.fbi.gov/news/press-releases/joint-statement-by-fbi-and-cisa-on-peoples-republic-of-china-activity-targeting-telecommunications?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=%5B1916549%5D-%2Fnews%2Fpress-releases%2Fjoint-statement-by-fbi-and-cisa-on-peoples-republic-of-china-activity-targeting-telecommunications.

² Robert Legare, et al, *Trump, Vance, Harris campaign potential targets in broad China-backed hacking operation*, CBS NEWS (Oct. 25, 2024), <https://www.cbsnews.com/news/trump-vance-potential-targets-china-backed-hacking-operation/>.

³ Ellen Nakashima, et al, *Chinese hackers said to have collected audio of American calls*, WASHINGTON POST (Oct. 28, 2024), <https://www.washingtonpost.com/national-security/2024/10/27/chinese-hackers-cellphones-trump/>.

⁴ *Id.*; Sarah Krouse, et al, *U.S. Wiretap Systems Targeted in China-Linked Hack*, WALL STREET JOURNAL (Oct. 5, 2024), <https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b>.

⁵ Krouse *supra* note 4.

⁶ Press Release, Sen. Charles E. 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

regarding a cyberattack on AT&T, which resulted in exposure to over 90 million Americans' data, potentially including federal agencies' communications patterns.⁷ I also wrote to CISA on July 3, 2024, regarding a recent cyberattack, which released "critical information about the operation of U.S. infrastructure."⁸ Additionally, on April 8, 2024, I wrote letters to seven of the Sector Risk Management Agencies responsible for overseeing our nation's critical infrastructure to highlight the threat of cyberattacks on our critical infrastructure sectors.⁹ It is imperative that our federal agencies work to ensure all data and critical infrastructure is safe and secure to prevent future attacks.

Unfortunately, this is not the first time U.S. foreign adversaries have hacked, or attempted to hack, into the devices and networks of current and former government officials. On August 10, 2024, Politico reported that starting on July 22, their office began receiving emails from an anonymous account with internal communications and information regarding vice presidential candidate and Senator J.D. Vance.¹⁰ The Trump Campaign, along with the FBI, Office of the Director of National Intelligence (ODNI), and CISA, confirmed that Iran hacked former President Trump's campaign.¹¹ Additionally, on July 17, 2024, NBC News reported that three former Trump officials have requested personal security details, to include protection from credible cyberattacks.¹² Without additional information from the government, it appears that our adversaries are becoming more brazen while the agencies tasked with our nation's security remain idle.

Accordingly, so Congress may conduct objective and independent oversight concerning the October 2024 Salt Typhoon cyberattacks and DHS, Secret Service, and CISA's ability to protect current and former government officials from cyberattacks by foreign adversaries, please provide answers to the following no later than November 15, 2024:

1. When and how did DHS and CISA become aware of the October 2024 Salt Typhoon cyberattacks? Provide all records.¹³

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>.

⁷ Press Release, Sen. Charles E. 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>.

⁸ 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.

⁹ Supra note 6. Grassley: *Federal Agencies Must Stop 'Dragging Their Feet' On Bolstering Cybersecurity Defense*.

¹⁰ Alex Isenstadt, *We received internal Trump documents from 'Robert.' Then the campaign confirmed it was hacked* (Aug. 10, 2024), POLITICO, <https://www.politico.com/news/2024/08/10/trump-campaign-hack-00173503>.

¹¹ Vaughn Hillyard & Alexandra Marquez, *Trump campaign says it was hacked by Iranian group*, NBC NEWS, (Aug. 10, 2024, 6:47 PM), <https://www.nbcnews.com/politics/2024-election/trump-campaign-says-was-hacked-iranian-group-rcna166098>; Press Release, CISA, *Joint ODNI, FBI, and CISA Statement* (Sep/ 18, 2024), <https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement>.

¹² Carol E. Lee and Ken Dilanian, *Ex-Trump officials say they asked the Biden DOJ for protection from Iranian threats but never got an answer* (July, 17, 2024), NBC NEWS, <https://www.nbcnews.com/investigations/ex-trump-officials-asked-biden-doj-protection-iran-threats-no-answer-rcna162301> (Victoria Coates, Matthew Pottinger, and Robert Greenway stated in a letter to the Justice Department, "It is clear there are specific, credible threats against us and our families by Iran and those inspired to act on Iran's behalf," the officials wrote in the letter, a copy of which they provided to NBC News. "This necessitates urgent steps to improve our physical and cyber security.")

¹³ "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).

2. Provide a complete list of government agencies, private businesses, current and former government officials, and private citizens affected by the attack.
3. Have all affected companies and victims been notified? If so, when were they notified? If not, why not?
4. What specific steps are DHS and CISA taking to secure government data and the data of current and former government officials, private citizens, and affected companies from future cyberattacks?
 - a. What role, if any, has the White House's Unified Coordination Group played in mitigating effects from the October 2024 cyberattacks and preventing future attacks?¹⁴ Provide all records.
 - b. Has the Cyber Safety Review Board initiated an investigation into Salt Typhoon? If not, why not?¹⁵
5. What security measures are currently in place by DHS, CISA, and Secret Service to protect former and current government officials who are currently under threat of a cyberattack? Describe those security measures.
6. Provide a list of credible cyber threats against current and former government officials that DHS, CISA, and Secret Service are aware of.

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

¹⁴ John Sakellariadis, *DHS to probe Chinese telco hacks that targeted Trump, Vance*, POLITICO (Oct. 27, 2024), <https://www.politico.com/news/2024/10/27/dhs-probe-china-telco-hack-trump-vance-00185733>.

¹⁵ *Id.* (quoting a DHS spokesperson stating the Board will “initiate a review of this incident at the appropriate time”).