Objection to Proceeding to the Nomination of Sean Plankey

Mr. WYDEN. Mr. President, I must object to the Senate proceeding to the nomination of Sean Plankey of Pennsylvania, to be Director of the Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security.

Since July 2022, I've repeatedly urged CISA to release an important, unclassified report by independent cybersecurity experts that the agency commissioned, titled "U.S. Telecommunications Insecurity 2022." Congress and the American people have a right to read this report, and until CISA releases it, I must object to this nomination.

CISA permitted my staff to read the report in person at the agency's office in the fall of 2023. However, CISA has marked this unclassified report "For Official Use Only" and has refused to provide copies of the report to Congress and in response to FOIA requests from the public. I directly asked then-CISA Director Jen Easterly to release the report in a February 27, 2024, phone call; however, she continued to stonewall my requests until she left office in January 2025.

CISA has to date refused to release the report by making a claim that the report is predecisional and deliberative, and protected by a so-called "deliberative process privilege." Setting aside that a FOIA exemption does not apply to disclosures to Congress, based on my staff's review of this report, this report is a technical document containing factual information about U.S. telecom security. The report does not recommend or discuss specific policy options that CISA could take to address this threat. As such, this report contains important factual information that the public has a right to see and CISA should stop withholding the entire report under a purported "deliberative process privilege" claim.

On February 29, 2024, I wrote to then-President Biden, urging the Administration to take action to address the serious national security threat posed by foreign governments exploiting U.S. phone carriers' weak cybersecurity. In that letter to then-President Biden, I stated that "CISA is actively hiding information about [the threat] from the American people…CISA refuses to publicly release this unclassified report, which includes details that are relevant to policymakers and Americans who care about the security of their phones." The Biden Administration took no action in response to my letter.

CISA's inaction on telecommunications security prompted the agency's top telecommunications security expert to file a whistleblower report with the Federal Communications Commission (FCC) in the summer of 2024. Citing his access to non-public reports and other "very concerning information," the CISA official told the FCC that "there have been numerous incidents of successful, unauthorized attempts to access the network user location data of communications service providers operating in the USA." He added that foreign surveillance went beyond

location tracking and included “the monitoring of voice and text messages” and “the delivery of spyware to targeted devices.”

CISA’s multi-year cover up of the phone companies’ negligent cybersecurity has real consequences. In a November 2024 joint statement, CISA and the Federal Bureau of Investigation confirmed that the Chinese government hacked “multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders.” Vice President Vance subsequently revealed that his communications and those of President Trump were compromised in this hack. This espionage incident, and the harm to U.S. national security caused by it, were the direct result of U.S. phone carriers’ failure to follow cybersecurity best practices, such as installing security updates and using multi-factor authentication, and federal agencies failing to hold these companies accountable.

The federal government still does not require U.S. phone companies to meet minimum cybersecurity standards. While it is too late to prevent the Salt Typhoon hack, there is still time to prevent the next incident. As such, I intend to object to considering this nominee until CISA agrees to release this report, which will enable Congress and the public to better understand the current threats and the need for stronger cyber defenses.