

## United States Senate

May 8, 2024

The Honorable Jen Easterly  
Director  
Cybersecurity and Infrastructure Security Agency  
U.S. Department of Homeland Security  
245 Murray Lane SW 950  
Washington, DC 20528

Dear Director Easterly:

I write today regarding the ongoing hacks by Russian state actors that have exposed sensitive federal communications and the concerning trend of cybersecurity failures within the federal government. As head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), I request your immediate attention and response to these grave concerns and threats to U.S. national security each of these incidents present.

Recently, Federal Bureau of Investigation (FBI) Director Christopher Wray issued grave [warnings about](#) the growing threat of cyberattacks to U.S. critical infrastructure by actors connected to the government of Communist China. While speaking at the 2024 Vanderbilt Summit on Modern Conflict and Emerging Threats, Director Wray stated that the Chinese Communist Party (CCP) is developing the, "ability to physically wreak havoc on our critical infrastructure at a time of its choosing," and that the CCP's plan is, "to land low blows against civilian infrastructure to try to induce panic." These threats against the critical infrastructure of the United States are incredibly disturbing given the issues the U.S. government continues to face in preventing intrusions and cyberattacks by malign foreign actors.

Following the SolarWinds hack by Russian state actors in 2020, the Biden administration touted federal funding and various executive actions to bolster our cybersecurity defenses and better protect against these attacks. These actions have clearly not been effective enough to stop two major cyberattacks from occurring in the last 10 months, one by Chinese actors and the other by Russian actors.

The Honorable Jen Easterly

May 8, 2024

Page Two

It is worrying that the administration's cybersecurity efforts appear to be more focused on colluding with Big Tech to [censor](#) the speech of law-abiding Americans, than it has been on preventing cyberattacks. The continued politicization of CISA represents a serious and dangerous misuse of government resources that should be 100% focused on its obligation to protect the cybersecurity of the U.S. government from foreign actors and holding commercial partners that have failed to meet our security standards accountable.

Last month, CISA's Cyber Safety Review Board (CSRB) released a [report](#) on the hack perpetrated by actors connected to the government of Communist China, saying that the hack was "preventable," and identifying a "series of Microsoft operational and strategic decisions that collectively pointed to a corporate culture that deprioritized enterprise security investments and rigorous risk management." The CSRB also held a classified briefing on this hack with the House of Representatives Committee on Homeland Security's Cybersecurity and Infrastructure Protection Subcommittee.

A week later, after this report was issued by CSRB, CISA issued an [emergency directive](#) related to the ongoing hack by Russian state actors stating that the hackers may have once again gained access to federal communications and requiring federal agencies to "analyze potentially affected emails, reset any compromised credentials, and take additional steps to secure privileged Microsoft Azure accounts."

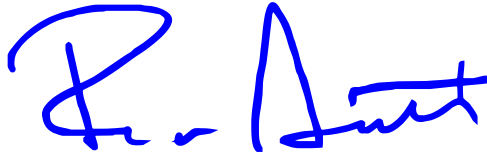
I am disturbed that companies which contract with the federal government to perform key, extremely sensitive services continue to be susceptible to hacks from foreign actors and that the persistent failures to prevent these attacks put our national security at risk. In the interest of transparency and accountability, I ask that you immediately respond to the following questions:

1. What progress has been made to address the security failures that led to the recent hacks by Chinese and Russian state actors?
2. What standards or benchmarks has CISA set for contractors to improve cybersecurity protocols and how often are these standards and benchmarks being evaluated?
3. What action has CISA taken to hold contractors accountable for failures to prevent cyberattacks which jeopardize the security of government networks and increase risks to U.S. national security?
4. Given that Russian actors have gained access to sensitive source code in their latest attack, how can CISA be certain that ongoing hacking activities are not further jeopardizing U.S. government networks?

The Honorable Jen Easterly  
May 8, 2024  
Page Three

I appreciate your prompt response and continued efforts to protect the U.S. government and the American people from cybersecurity threats.

Sincerely,

A handwritten signature in blue ink, appearing to read "Rick Scott". The signature is stylized with a large initial "R" and a prominent "S".

Rick Scott  
United States Senator