

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5051
MINORITY (202) 225-5074
<https://oversight.house.gov>

March 24, 2021

President Joseph R. Biden, Jr.
The White House
1600 Pennsylvania Avenue
Washington, D.C. 20500

Dear President Biden:

It has been an honor to work closely with your Administration to deliver the American Rescue Plan, which will mean life instead of death for countless Americans and recovery instead of recession for Main Street economies. As part of this effort, the Committee on Oversight and Reform worked closely with the Committee on Homeland Security and our Senate counterparts to provide \$2 billion for federal information technology cybersecurity and modernization to streamline and strengthen our networks in the face of escalating cyberattacks that threaten our pandemic response efforts and national security. To maximize the effectiveness of this funding and to make urgently needed progress on critical cybersecurity vulnerabilities, I ask that you prioritize immediate action on the new authority granted by the fiscal year 2021 National Defense Authorization Act to nominate a National Cyber Director.

The mission-critical importance of nominating a National Cyber Director was highlighted at a hearing I held this month on the Government Accountability Office (GAO) 2021 High-Risk Report. The report revealed that, shockingly, more than 750 of GAO's recommendations to address the federal government's cybersecurity challenges remain unaddressed—500 of which have accumulated since the Trump Administration eliminated the role of White House Cybersecurity Coordinator in May of 2018.¹

The lack of centralized and coordinated cybersecurity leadership at the White House has had devastating consequences, as recently demonstrated by the SolarWinds breach in which a suspected Russian state actor infiltrated the networks of at least nine federal agencies and over a hundred private-sector companies.² As we discussed in a joint hearing on the breach with the Committee on Homeland Security in February, our attackers were left undiscovered for months

¹ Government Accountability Office, *GAO's 2021 High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas* (GAO-21-119SP) (Mar. 2, 2021).

² The White House, *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger* (Feb. 17, 2021) (online at www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/).

to move silently throughout our federal networks and steal information about our nation’s inner workings. The full extent of the breach is still under investigation and may never be fully understood.³

In his testimony before the Committee, Comptroller General Gene Dodaro confirmed that having a statutory cyber coordinator in place in the White House would have been one of the most important factors in detecting, responding to, or possibly even preventing the SolarWinds attack. Among other things, this position could have been instrumental in ensuring agencies across the federal government had best practice criteria in place to mitigate IT supply-chain weaknesses—the very vulnerabilities that were exploited by the SolarWinds breach. The Comptroller General testified that, had the GAO recommendations been addressed, “we would have been better postured to detect the attack ourselves—to take quicker action.”⁴

On the day of our hearing with Comptroller General Dodaro, Microsoft announced a massive breach of its Exchange Server that compromised at least 30,000 U.S. organizations. Reports attributed the original breach to a group of hackers connected to China but warned that at least ten different groups rushed in to exploit the vulnerability for espionage purposes.⁵ We applaud the work of the National Security Council in convening an interagency task force to address this matter, and the exemplary skill and leadership of Anne Neuberger in responding to the SolarWinds and Microsoft Exchange attacks in her role as Deputy National Security Adviser for Cyber and Emerging Technology. However, the robust statutory authority and resources of the National Cyber Director role and supporting office were developed with precisely these kinds of complex challenges in mind and should be utilized to their fullest extent as soon as possible.

This high-risk area is so critical, complex, and concerning that, today, GAO issued a follow-up report on the lack of progress that has been made on four major cybersecurity challenges: establishing a comprehensive cybersecurity strategy and performing effective oversight, securing federal systems and information, protecting critical infrastructure, and protecting privacy and sensitive data.⁶ The report confirms that, once the National Cyber Director position is filled, “the federal government will be better situated to direct activities to overcome the nation’s cyber threats and challenges, and to perform effective oversight.”⁷

The Trump Administration’s elimination of the White House Cybersecurity Coordinator role in 2018 left the nation more vulnerable, and the need for comprehensive, streamlined,

³ Committee on Oversight and Reform, *Press Release: Oversight and Homeland Security Committees Discussed Next Steps for Government and Private Tech Following SolarWinds Breach* (Feb. 26, 2021) (online at <https://oversight.house.gov/news/press-releases/oversight-and-homeland-security-committees-discussed-next-steps-for-government>).

⁴ Committee on Oversight and Reform, *Hearing with Comptroller General of the United States Gene L. Dodaro*, 117th Cong. (Mar. 2, 2021).

⁵ *The Cybersecurity 202: More Hackers Jump to Take Advantage of a Widespread Microsoft Security Flaw*, Washington Post (Mar. 11, 2021) (online at www.washingtonpost.com/politics/2021/03/11/cybersecurity-202-more-hackers-jump-take-advantage-widespread-microsoft-security-flaw/).

⁶ Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges* (GAO-21-288) (Mar. 24, 2021).

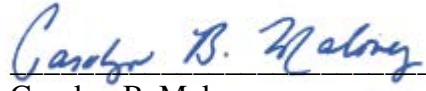
⁷ *Id.*

President Joseph R. Biden, Jr.

Page 3

effective federal cybersecurity leadership has never been greater. Congress and the executive branch must work together strategically on cybersecurity so federal agencies are in the best position possible to serve the American people through this time of crisis, and that means nominating and confirming the nation's first National Cyber Director as soon as possible.

Sincerely,

A handwritten signature in blue ink that reads "Carolyn B. Maloney". The signature is written in a cursive style and is positioned above a horizontal line.

Carolyn B. Maloney

Chairwoman

cc: The Honorable James Comer, Ranking Member