

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

April 5, 2021

Mr. Christopher DeRusha
Federal Chief Information Security Officer
Office of Management & Budget
Washington, D.C. 20500

Dear Mr. DeRusha:

Thank you for your recent testimony before the Committee on Homeland Security and Governmental Affairs as part of the Committee's investigation into the SolarWinds Orion hack, Microsoft Exchange server hacks, and other recent cyberattacks. A recent report has raised the troubling possibility that some federal agencies did not fully report the extent of the SolarWinds breach to Congress.¹

As our hearing highlighted, there is no easy solution to advanced persistent cyber threats. Time and again this Committee has discussed the challenges of defending against sophisticated, well-resourced, and patient cyber adversaries.² Nevertheless, the fact remains that despite significant investments in cyber defenses, the federal government did not initially detect this cyberattack. We appreciate your testimony on this issue, along with that of your colleagues, raising important questions about our national and federal cybersecurity strategy.

A layered and holistic federal cybersecurity strategy is key to a comprehensive federal cyber deterrence and defense capability. An effective federal cybersecurity strategy will need to reevaluate core assumptions and consider new solutions and approaches to cybersecurity. For example, it may be appropriate to assume some level of compromise within networks and implement a zero-trust network architecture, improve protection at end points complemented by heuristic and behavior-based detection capabilities, and regularly deploy hunt teams to seek out malicious actors. Mitigating vulnerabilities and reducing legacy information technology that serve as open doors to malicious hackers is also important. So will be deterrence efforts that create real-world consequences for cyber-attacks against the United States—investigation,

¹ Alan Suderman, ASSOCIATED PRESS, *AP sources: SolarWinds hack got emails of top DHS officials* (March 29, 2021), available at <https://apnews.com/article/rob-portman-hacking-email-russia-8bcd4a4eb3be1f8f98244766bae70395>.

² E.g., *Under Attack: Cybersecurity & the OPM Data Breach: Hearing Before the S. Comm. on Homeland Security & Governmental Affairs*, S. Hrg. 114-449 (June 25, 2015) (Statement of Dr. Andy Ozment, Ass't Secretary for Cybersecurity & Communications, Dep't of Homeland Security); SEN. TOM COBURN, RANKING MEMBER, S. COMM. ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS, A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY'S MISSIONS AND PERFORMANCE 97 (Dec. 2015) (quoting Suzanne E. Spaulding, former Under Secretary of National Protection & Programs, Dep't of Homeland Security, "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth.").

Mr. Christopher DeRusha

April 5 2021

Page 2

attribution, prosecution, and sanctions. At the national level, our cybersecurity strategy will require careful consideration of the appropriate role of the federal government, companies, and citizens in cyber defense, especially when it comes to nation-state actors with near unlimited resources and time.

Also important to our federal cybersecurity strategy is defined structures for inter-agency coordination on incident response. At our hearing, we discussed the numerous entities with potentially overlapping responsibilities related to federal cybersecurity. It is important that there be a single point of accountability for leading response efforts to prevent confusion and duplication. We are concerned this level of accountability is currently lacking.

We look forward to working with the Administration on needed improvements to the Federal Information Security Modernization Act of 2014, and other legislative improvements to defend better against advanced persistent cyber threats. To assist us in this investigation and these policy considerations, please provide unredacted copies of the following documents no later than 5:00 p.m., April 20, 2021:

1. The current federal cybersecurity strategy and any associated implementation plan(s) and a description of any plan to update the strategy or plan(s).
2. A list of roles and responsibilities for federal cybersecurity including an assessment of how these defined roles prevent duplicative efforts and facilitated the federal government's response to the SolarWinds attack.
3. Documents sufficient to show the specific information systems compromised or targeted at federal agencies in the SolarWinds Orion attack and Microsoft Exchange attacks; the names of the individuals whose accounts or systems were compromised or targeted if at the SES, ES, or equivalent level; and the agencies, programs, and teams with which those individuals and systems were associated, to the greatest level of detail possible.
4. Documents sufficient to show current and planned metrics used to measure security in accordance with section 3554 of title 44, United States Code.
5. Cyberscope data received for each department or agency for FY 2020.

The Committee is authorized by Rule XXV of the Standing Rules of the Senate and S. Res. 70 to investigate "the efficiency and economy of all branches of the Government . . ." and is the primary Committee of jurisdiction in the United States Senate for federal cybersecurity.

Many of the documents requested should be readily available to the Department. As such, please begin production of documents immediately and do not delay productions for the purpose of including a cover letter. We request a letter only at the conclusion of the production to certify completeness. Classified information should be provided under separate cover via the Office of Senate Security. Additionally, we request your office provide a briefing to discuss the documents provided, after providing those documents.

Mr. Christopher DeRusha

April 5 2021

Page 3

Thank you for your prompt attention and cooperation in this matter. These documents and information will help the Committee in considering potential legislation to improve federal cybersecurity, including reforms to the Federal Information Security Modernization Act of 2014. If you have any questions about this request, please contact Christopher Mulkins at (202) 228-1346 for Chairman Peters and Liam McKenna at (202) 228-0079 for Ranking Member Portman.

Sincerely,



Gary C. Peters
Chairman



Rob Portman
Ranking Member