

United States Senate

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

DAVID M. WEINBERG, STAFF DIRECTOR
PAMELA THIESSEN, MINORITY STAFF DIRECTOR
LAURA W. KILBRIDE, CHIEF CLERK

April 5, 2021

Mr. Brandon Wales
Acting Director, Cybersecurity & Infrastructure Security Agency
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Wales:

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 the Department of Homeland Security (DHS or the Department) 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.").

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.

Our hearing also revealed key limitations of the EINSTEIN intrusion detection and intrusion prevention system. EINSTEIN is a signature-based intrusion detection and prevention system that sits on the perimeter of civilian federal agencies' computer networks.³ As you alluded to in your testimony, network perimeters are increasingly irrelevant with modern information technology infrastructure that emphasizes end-to-end encryption and reliance on cloud service providers outside of an organization's network; these technologies represent an inherent limitation of perimeter-based intrusion detection systems like EINSTEIN.⁴ Additionally, signature-based intrusion detection and intrusion prevention systems are largely limited to detecting previously seen threats—they are ineffective at identifying or blocking sophisticated and novel attacks like the SolarWinds hack. As this Committee warned nearly five years ago, "Current reliance on decades old signature-based detection technology limits the effectiveness of EINSTEIN against advanced persistent threats."⁵

The authorization for DHS to operate EINSTEIN lapses on December 18, 2022 and we look forward to working with you to determine whether and how to reauthorize the program to address these limitations and, more broadly, how 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. on April 20, 2021:

1. Documents sufficient to show the specific information systems compromised at federal agencies shared with CISA in regards to the SolarWinds and MS Exchange cyberattacks or that may have been captured by EINSTEIN in the past six months, including the names of the individuals whose accounts or systems were compromised or targeted if at the SES, ES, or equivalent level; and the agencies and programs with which those individuals and systems were associated, to the greatest level of detail possible.
2. The Department's current cybersecurity strategy and implementation plan⁶ and intrusion assessment plan.⁷

³ S. Rept. 114-378.

⁴ *E.g.*, NAT'L INST. OF STANDARDS & TECHNOLOGY, NAT'L CYBERSECURITY CENTER OF EXCELLENCE, ZERO TRUST ARCHITECTURE, <https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture> ("The proliferation of cloud computing, mobile device use, and the Internet of Things has dissolved traditional network boundaries. Hardened network perimeters alone are no longer effective for providing enterprise security in a world of increasingly sophisticated threats.").

⁵ S. Rept. 114-378.

⁶ Homeland Security Act of 2002 § 2211(a), (d).

⁷ Homeland Security Act of 2002 § 2210(b)(1).

3. Documents sufficient to show the current and planned technical capabilities of EINSTEIN 1 (E1); EINSTEIN 2 (E2); EINSTEIN 3 Accelerated (E3A); and Enhanced Cybersecurity Services, including any improvements, new technologies, modification of existing technologies, advanced protective technologies, or detection technologies beyond signature based detection planned, acquired, tested, evaluated, piloted, or deployed on the EINSTEIN platform.⁸
4. All reports, evaluations, studies, or reviews related to EINSTEIN classified indicators, including the assessment CISA performed in 2020 on the efficacy of utilizing classified indicators and any update since the publication of that study.
5. All classified indicators in use on E3A as of the date of this letter as well as any contextual information DHS has regarding those indicators.
6. Documents sufficient to show the current and planned technical capabilities of the Continuous Diagnostics and Mitigation (CDM) program including advanced network security tools to improve visibility of network activity and to detect and to mitigate intrusions and anomalous activity,⁹ and the current plan to ensure that each agency utilizes advanced networks security tools as part of the CDM program.¹⁰
7. The performance work statement for each CDM integrator including for each: documents sufficient to show whether the contract is fixed price or cost based and incentives and awards.
8. Operations and spending plans for the National Cybersecurity Protection System and for the CDM program to the greatest level of detail possible for the each of the past five fiscal years.

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 operations 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 as soon as possible 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 CISA provide briefings to discuss its cybersecurity programs and the documents provided, after providing those documents.

⁸ Homeland Security Act of 2002 §§ 2312(b)(4)–(5), 2313(b)(2).

⁹ Federal Cybersecurity Enhancement Act of 2015 § 224(a).

¹⁰ Federal Cybersecurity Enhancement Act of 2015 § 224(b).

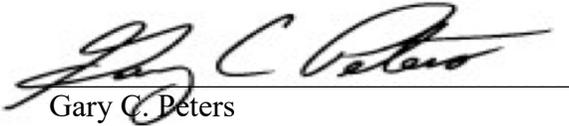
Mr. Brandon Wales

April 5, 2021

Page 4

Thank you for your prompt attention and cooperation in this matter. These documents and information will help us in considering potential reauthorization language for the National Cybersecurity Protection System. 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