RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

February 19, 2021

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

Dear Acting Director Wales:

I write to seek information about the policy failures that contributed to the U.S. government's inability to detect and prevent a major Russian hacking campaign against U.S. government agencies and U.S. companies. I am particularly concerned that the government's $6 billion EINSTEIN cybersecurity system failed to promptly detect the hacks even years after warnings about EINSTEIN's vulnerability to such a campaign.

On December 13, 2020, Microsoft and FireEye revealed the existence of a hacking campaign that has since been linked to the breach of nine U.S. agencies as well as approximately 100 companies. The initial hacking vector was a backdoor in Orion, a commercial network monitoring tool created by SolarWinds, a U.S.-based software company. The U.S. government subsequently attributed this hacking operation to a threat actor who is "likely Russian in origin."

The malware was split into several pieces, according to a detailed forensic report published by the Cybersecurity and Infrastructure Agency (CISA). The first stage was smuggled into victims' networks as part of an update to SolarWinds' software. This backdoor was programmed to lay dormant for at least two weeks, after which it attempted to call home and download the malware's second stage, which enabled the hackers to take control and begin to ransack their victims' networks.

The downloading of the second stage of the malware was essential to the success of this hacking campaign. If the malware could not call home to download the second stage — for example, because the server running SolarWinds' software was either not connected to the internet or was protected by a firewall — the hackers would have been unable to gain access using the backdoor. And, even if the download of the second stage were successful, the hackers risked discovery should cyber defensive systems deployed by the government detect it. In this case, the malware contacted an internet domain specially created for the campaign, which no U.S. government server had reason to contact. However, CISA and other federal cybersecurity defenders did not detect the hack in progress, or even discover it weeks after federal agencies were hacked. Instead, FireEye revealed the hacking campaign in December 2020 after discovering the hackers in its own corporate network.

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326–7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431–0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962–7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858–5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330–9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589–4555

HTTPS://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

Since 2003, the government has operated a cybersecurity defensive system called EINSTEIN to detect and thwart hacks of federal systems. Under this program, which has cost taxpayers more than $6 billion to date, CISA collects and analyzes metadata about all data going in and out of civilian federal agency networks. EINSTEIN was initially designed to only detect known threats — that is, to detect the reuse of malware or servers that the government or its partners had previously identified. This meant that EINSTEIN was unable to detect hacking campaigns using novel malware and fresh servers that had not been used in previous hacking campaigns. While it is certainly easier for hackers to reuse malware and other infrastructure between operations, many of our adversaries have the resources, tradecraft, and patience to create new hacking tools and rent new servers for each major operation.

However, in January 2016, the Government Accountability Office (GAO) issued a report warning EINSTEIN lacked the capability to detect hackers using novel malware and servers not previously associated with hacking campaigns and recommended that the Department of Homeland Security (DHS) assess the feasibility of adding this functionality. In an updated report published in December 2018, GAO wrote that DHS "determined that enhancing [EINSTEIN]'s current intrusion detection approach to include functionality that would detect deviations from normal network behavior baselines would be feasible. In addition, according to DHS officials, the department was operationalizing functionality intended to identify malicious activity in network traffic otherwise missed by signature-based methods."

CISA has not provided any public update on its efforts to upgrade EINSTEIN, however, the system clearly failed to detect the Russian malware calling home for further instructions. Five years after GAO identified a major gap in the government's cybersecurity defenses, CISA and its EINSTEIN system remain incapable of protecting federal networks from careful adversaries. That is, by using bespoke malware and clean servers, Russian hackers were able to bypass CISA's defenses and ransack federal networks for months without detection.

Russia's hacking of numerous federal agencies using the SolarWinds backdoor is a national security disaster. Congress has a responsibility to determine why the agencies that were hacked did not have properly configured firewalls — a technology from the 1990s — defending their servers running SolarWinds Orion and why CISA's $6 billion EINSTEIN cyber defense system did not detect the download of the malware's second stage. Accordingly, please provide us with unclassified answers to the following questions by March 23, 2021:

1. The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have both published guidance related to the configuration of firewalls. NSA recommends that Information Technology administrators "only allow traffic that is required for operational tasks; all other traffic should be denied." NIST recommends that "Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic." Does CISA agree with this guidance from NSA and NIST?

2. Does CISA have the authority to require agencies to configure their firewalls to block outgoing connections from agency servers, except where there is an operational need for

a particular agency server to initiate connections to other servers on the internet? If yes, has CISA done so? If CISA has not done so, please explain why.

3. SolarWinds' CEO informed my office in a recent briefing that there was no need to permit servers running SolarWinds' Orion software to connect to any unknown server on the internet and that the functionality provided by allowing the SolarWinds Orion software to contact solarwinds.com was limited. Does CISA agree that the SolarWinds malware could have been neutralized had victim agencies placed firewalls in front of the servers running SolarWinds Orion and configured them to block outgoing connections to the internet?

4. CISA has long recommended that agencies segment and segregate their internal networks, which makes it more difficult for intruders to move around and gain access to an organization's most sensitive information. What percentage of federal agencies subject to CISA's cybersecurity authority have implemented this advice?

5. According to the aforementioned December 2018 GAO report, CISA was working to add functionality to EINSTEIN to identify malicious activity in network traffic otherwise missed by signature-based methods. Please detail the status of this effort and, if it is already fully operational, please explain why CISA failed to detect the SolarWinds backdoor calling home to avsvmcloud.com.

6. Is CISA aware of any other U.S. government agencies that have successfully deployed technology capable of detecting deviations from normal network behavior? If so, please detail the steps taken by CISA to learn from those other agencies.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator