U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

June 3, 2021

The Honorable Ron Wyden
United States Senate
Washington, DC 20510

Dear Senator Wyden:

Thank you for your letter regarding the 2020 SolarWinds supply chain cybersecurity compromise and the role the EINSTEIN cybersecurity system plays in protecting our Federal networks and in detecting intrusions like we experienced during the SolarWinds breach.

We apologize for the delayed response and appreciate your continued support for the mission of the Cybersecurity and Infrastructure Agency (CISA).

While I will address each of the questions your letter poses in turn, I wanted to first provide additional information regarding the SolarWinds compromise and the EINSTEIN program that I feel will be beneficial to understanding how the program works and fits into CISA's larger suite of cyber security tools.

As you know, late last year, CISA became aware of a broad cyber intrusion campaign, largely associated with the supply chain compromise of SolarWinds Orion network management software. Nearly 18,000 entities were potentially exposed to the malicious SolarWinds software. CISA estimates a much smaller number were compromised when the threat actor activated the malicious backdoor they had installed in the SolarWinds product and moved into the exposed network.

Once inside the network, the actor was able to use their privileged access to abuse the authentication mechanisms – the systems that control trust and manage identities – ultimately allowing them to access and exfiltrate email and other data from compromised networks and Microsoft Office 365 cloud environments.

The primary objective of the threat actor in this campaign appears to be gaining access to sensitive but unclassified communications, and to identify additional opportunities to compromise IT supply chains.

As we respond to and mitigate the impacts of these incidents, we are also looking ahead to ensure that CISA is appropriately postured to defend today and secure tomorrow. To this end, we are focused on urgent improvements to increase CISA's visibility into cybersecurity risks across the federal civilian executive branch. Additionally, we must increase and improve our insight into agency cloud environments and endpoints across non-federal entities where feasible. To achieve this goal, we must provide agencies with critical detection tools and build our capacity to

analyze increasing volumes of security data. While no organization can prevent every cyber intrusion, increased visibility will allow us to detect and respond to incidents more quickly, thereby limiting harm to victim organizations.

To this end, CISA has developed the National Cybersecurity Protection System (NCPS) which is an integrated system-of-systems that delivers a range of capabilities, such as intrusion detection, analytics, information sharing, and intrusion prevention. These capabilities provide a technological foundation which enables CISA to secure and defend the Federal Civilian Executive Branch (FCEB) agencies' information technology infrastructure against advanced cyber threats. NCPS includes the hardware, software, supporting processes, training, and services that the program acquires, engineers, and supports to fulfill the agency's cybersecurity mission.

One of CISA's key technologies within NCPS is EINSTEIN, one of many tools and capabilities that assist in federal network defense. The goal of the NCPS EINSTEIN set of capabilities is to provide the Federal Government with an early warning system, improved situational awareness of intrusion threats to FCEB networks, near real-time identification of malicious cyber activity, and prevention of that malicious cyber activity.

EINSTEIN cannot be thought of as a separate offering, rather it must be thought of as part of CISA's cohesive and holistic strategy to protect federal civilian agencies. Moreover, EINSTEIN must be thought of as an intrusion detection system, looking at the perimeter of a network and examining traffic that is coming from outside the network to inside the network and not designed to detect an unknown threat like the SolarWinds attack. However, what the SolarWinds compromise did reveal is that EINSTEIN must be supplemented with capabilities that enable us to look inside the network to better detect in-network intrusions.

For this reason, CISA is urgently moving our detecting capabilities from the perimeter layer into agency networks to better focus on the end-point security of items such as servers and workstations where adversaries are most active today, which is an approach consistent with leading trends in the cybersecurity industry as adopted by public and private organizations. The additional $650 million dollars included in the American Rescue Act will enable CISA to rapidly accelerate the transition from a perimeter defense construct to a construct whereby the agency will be able to identify threat activity within agency networks in real-time.

With respect to your specific questions,

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?**

   Yes, CISA agrees with the guidance published by NIST and NSA regarding firewall

policies.

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.**

   Under the Federal Information Security Modernization Act (FISMA), CISA's authorities include coordinating government-wide efforts on information security policies and practices, and developing and overseeing the implementation of information security-related binding operational directives to other agencies. 44 U.S.C. §§ 3553(b), (f)-(h); 6 U.S.C. § 663. It would be impractical for CISA to direct individual agencies to adopt specific network and device configurations on a broad scale, particularly given the unique operational requirements of each agency. However, CISA is continuously evaluating opportunities to use binding operational directives or other authorities to drive appropriate security measures, including to adopt risk-based configuration practices.

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?**

   CISA agrees that a firewall blocking all outgoing connections to the internet would have neutralized the malware. While CISA did observe victim networks with this configuration that successfully blocked connection attempts and had no follow-on exploitation, the effectiveness of this preventative measure is not applicable to all types of intrusions and may not be feasible given operational requirements for some agencies.

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?**

   CISA does not presently have data regarding the percentage of agencies that have segmented and segregated their internal networks. CISA continues to develop and promulgate guidance to encourage network segmentation, including to drive adoption of zero trust architectures.

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.

For background, NCPS includes the EINSTEIN set of sensor capabilities, including: EINSTEIN 1, which provides network traffic flow monitoring services; EINSTEIN 2, which provides intrusion detection services; and EINSTEIN 3 Accelerated (E3A), which provides intrusion prevention services. CISA utilizes the EINSTEIN platform to conduct intelligence-based threat hunting for Federal Civilian Executive Branch (FCEB) entities. Detection and prevention measures are sourced from open-source, proprietary, and classified threat intelligence sources and subsequently used to identify malicious activity at the network boundary. While the SolarWinds intrusions were ongoing, there were no as-of-yet known network-based prevention and detection indicators to identify this activity. This was true for the entire community of network defenders, including CISA. However, once indicators of compromise where identified from CISA's incident response engagement and industry sources, CISA was able to use EINSTEIN 1 to identify potentially compromised agencies.

CISA leverages a capability to utilize artificial intelligence and machine learning techniques with network-based data to identify suspicious malicious traffic. This capability is deployed at two Internet Service Provider (ISP) locations and within the E3A architecture known as the Nest. Like many such tools, this capability is limited in its ability to detect verifiable malicious network-based activity. It bears noting that commercial capabilities using non-signature-based detection techniques were similarly unable to detect the SolarWinds intrusions at government and private sector victims.

More broadly, CISA is urgently adapting our cybersecurity programs, including EINSTEIN, to address changes in the technology and risk environments. For example, with the increased use of encrypted traffic entering and exiting federal networks, which provides privacy and security benefits, the EINSTEIN 2 technology that was designed to address risks and technology a decade ago no longer provides the visibility that CISA needs.

Accordingly, CISA is urgently moving its detection capabilities from perimeter layer into agency networks to better focus on endpoint security. This approach is consistent with leading trends in the cybersecurity industry as adopted by public and private organizations. The additional $650 million dollars included in the American Rescue Act will enable CISA to rapidly accelerate the transition from a perimeter defense construct to a construct whereby agencies and CISA will be better situated to identify threat activity within federal networks in near-real-time.

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.**

CISA is not aware of other U.S. government agencies, or private sector actors, that have

successfully deployed technology capable of detecting deviations from normal network behavior that would have been successful in detecting or preventing the SolarWinds incident.

CISA is working to address longer-term gaps in federal cybersecurity, such as identifying outdated systems, indefensible architectures, or inadequate focus on system maintenance, which are barriers to adopting modern cybersecurity technology and achieving consistent cyber hygiene. In order to raise the baseline for federal cybersecurity, CISA provides agencies with shared services and cybersecurity tools and training through the Quality Service Management Office and the Continuous Diagnostics and Mitigation program.

Both the Microsoft Exchange vulnerabilities and the SolarWinds campaign highlight the lengths to which sophisticated adversaries will go to compromise our networks. They will use never-seen-before techniques, exquisite tradecraft and zero-day vulnerabilities, to defeat our current cybersecurity architecture.

Knowing that, we must ensure the development of a modern cybersecurity governance structure and capabilities. We need cybersecurity tools and services that provide us a better chance of detecting the most sophisticated attacks. And we need to rethink our approach to managing cybersecurity across 101 Federal Civilian Executive Branch agencies.

Thank you again for your letter. Should you wish to discuss this further, please do not hesitate to contact me my office at 202-839-0907.

Sincerely,

Brandon Wales
Acting Director