STATEMENT OF

JANET VOGEL

CHIEF INFORMATION SECURITY OFFICER

DEPARTMENT OF HEALTH AND HUMAN SERVICES

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

UNITED STATES SENATE

AT A HEARING ENTITLED

"PREVENTION, RESPONSE, AND RECOVERY: IMPROVING FEDERAL CYBERSECURITY POST-SOLARWINDS"

PRESENTED

MAY 11, 2021

Thank you, Chairman Peters, Ranking Member Portman, and Members of the Committee, for the opportunity to provide remarks on the response by the Department of Health and Human Service (HHS) to recent cybersecurity incidents such as SolarWinds and to share lessons learned to mitigate future sophisticated cyber-attacks against the federal government and private sector.

The SolarWinds event represented an unprecedented attack on the vendor, SolarWinds corporation, and its public and private sector customers. Malicious actors accessed the SolarWinds environment and introduced malicious code, which they propagated to SolarWinds customers through regular software updates. These actors had access to as many as 18,000 customer environments through these updates. Based on publicly available information, experts estimated that most of the affected victims were private-sector companies, although the impact on the government was significant.

While HHS did identify affected SolarWinds products, we were able to remove those devices from production before they were "triggered" and had the opportunity to compromise HHS networks and data. The strength of HHS's incident response and remediation processes—combined with our experience and expertise—enabled research and forensics teams to mitigate risks associated with the SolarWinds compromise. This event allowed us to practice our incident response protocols and identify several lessons learned to strengthen our robust cybersecurity defenses.

Furthermore, SolarWinds revalidated an essential strategy to address this and future threats. Communication, collaboration, and coordination across the Federal government in association with trusted partners such as the Cybersecurity and Infrastructure Security Agency (CISA)

provides the needed exchange of vital information that allowed the Department to ensure that the IT environments across our vast agency remained secure and stable.

Notification and Resulting Prompt Actions to Mitigate the Threat

HHS quickly and efficiently reacted to the SolarWinds event within a few hours of notification. The Department implemented the requirements mandated by CISA in *Emergency Directive (ED) 21-01, Mitigate SolarWinds Orion Code Compromise.* HHS scanned for malware on SolarWinds products, consistent with information and guidance from the vendor and CISA. HHS did not detect the execution of that malware or any compromise or exfiltration of data, and we determined that no information was accessed or compromised via SolarWinds.

More specifically, HHS took the following decisive actions:

- **December 13, 2020:** HHS became aware that a supply chain attack was using SolarWinds Orion business software updates to distribute malware. HHS promptly used this information to analyze HHS enterprise security tools for activity matching the attack's indicators and tactics, techniques, and procedures. On the same day, HHS received ED 21-01 and immediately took steps to communicate information related to the required actions across the Department.

- **December 14, 2020 to December 16, 2020:** HHS provided status updates to CISA. In this time, HHS reported that all instances of SolarWinds Orion were removed from its network.

- **December 21, 2020 to January 6, 2021:** CISA issued multiple updates of the Supplemental Guidance and alerts that included new information on initial access vectors, updated mitigation recommendations, and new indicators of compromise (IOCs).

- **January 19, 2021 to January 25, 2021:** HHS submitted to CISA two required ED 21-01 status reports in response to the Supplemental Guidance version 3.

Information provided by DHS and other entities enabled HHS to quickly identify the effects of the attacks and to avert threats before malicious actors could exploit them. HHS utilized the tools and guidance provided by CISA across the Department to ensure a coordinated approach. We regularly engaged with CISA on eviction guidance for affected networks and shared corresponding resources across our agency.

Mitigating the Impact of SolarWinds

HHS has confirmed that it completed the required validation tasks for ED 21-01. We identified several SolarWinds instances in our environment, and all affected products were powered down and removed from production. To our knowledge, none of those affected products were activated to compromise or exfiltrate HHS information. As a result, HHS properly evaluated that, because the compromise of systems and the unauthorized access to information were limited, they did not impair national security. The Department also determined that the event did not meet the criteria of a "major incident" per the guidance of the Office of Management and Budget (OMB). An incident is major if there is a compromise of personally identifiable information (PII) of 100,000 or more people or, if realized, the incident is likely to result in demonstrable harm to the country and its people. We determined that neither of these criteria was met and did not declare a major incident.

Collaboration with Key Federal and Private Sector Partners

The SolarWinds event highlighted the importance of interagency collaboration to effectively respond to and recover from cyber threats. For example, HHS followed all guidance developed and issued by CISA, as articulated in ED 21-01. Consistent with that guidance, HHS immediately removed all affected SolarWinds products from production and terminated internet connectivity to those devices. The Department ensured that the agency's research and forensics staff thoroughly evaluated affected devices, and the Department is committed to ongoing and longer-term monitoring and reporting.

HHS is also the sector-specific agency for the Healthcare and Public Health (HPH) Sector, as defined in Presidential Policy Directive-21 (PPD-21). HPH Sector entities were notified through the Health Sector Cybersecurity Coordination Center (HC3)—an HHS organization that reports to the HHS CISO (Chief Information Security Officer) and advises the HPH sector of cybersecurity threats—in collaboration with the HHS Assistant Secretary for Preparedness and Response (ASPR) and its Critical Infrastructure Protection (CIP) team, as well as CISA. Together we provide insight and guidance to the sector regarding SolarWinds.

HHS also shared information with other healthcare delivery agencies—the Department of Veterans Affairs (VA) and the Defense Health Agency (DHA)—through HHS's Health Threat Operations Center (HTOC). The HTOC, which also reports to the HHS CISO, complements HC3's effort to share cybersecurity threats with private sector healthcare delivery organizations. Finally, other entities such as the Office of Management and Budget (OMB) and the National Security Council (NSC) have contacted HHS for additional information about the SolarWinds event. HHS's standard practice is to notify CISA within one hour of detecting an incident; in general, we may also notify HHS's OMB desk officer.

Lessons Learned Going Forward

During the investigating and remediating of threats posed by the SolarWinds event, HHS identified several lessons learned. Because cyber threats are dynamic, these are in the form of general principles to guide future responses rather than in the form of specific recommended actions:

- **Greater levels of redundancy in software and hardware assets may make it easier for the Department to change operating procedures in the event of a compromise.** HHS removed networking hardware from production, leaving organizations to develop workaround solutions. Greater levels of redundancy may offset the risk and effort associated with taking hardware and software offline.

- **Appropriate network segmentation and other defense-in-depth practices limit the degree to which a compromise of one system can spread to other systems.** HHS and its operating divisions value the access to and flow of data across the organization to fulfill the Departmental mission. However, to the greatest extent possible, protections must be in place to secure networks and information systems against attack, including movement across the network during a compromise.

- **Swift mobilization of both research and forensics and incident response teams across the organization is essential.** Quick action and collaboration within and among HHS operating divisions are necessary to identify, remove, and remediate threats before they can do significant damage to the Department. Similarly, information sharing and collaboration across these teams—and the Department—is vital. Information-sharing platforms and technologies centralize and organize information important to threat identification and remediation.

- **HHS and federal agencies should examine the benefits of leveraging a diverse set of tools to potentially lessen the impact if they are compromised.** The SolarWinds event underscored the potential damage that can be done when one widely used technology is exploited. HHS and other federal agencies should examine the potential benefit of leveraging a diverse set of tools, providing broader capabilities and lessens the impact should one tool be compromised.

- **HHS and government-wide supply chain governance and risk management may reduce threats and enable quicker recovery.** HHS has in place several mechanisms to evaluate software and hardware purchases before implementation. Using oversight processes, such as those required by the Federal Information Technology Acquisition Reform Act (FITARA), to better understand the prevalence and security of tools being requested allows HHS to make wiser decisions about which technologies to use. Similarly, studying the supply chain at the government-wide level and with respect to the technologies most commonly used across the government could yield practices and standards that HHS could employ to protect its IT environment. HHS already developed its Policy for Cyber Supply Chain Risk Management (C-SCRM), August 2020, that requires the Department and its operating divisions to identify and describe Information and Communications Technology (ICT) supply chains involved in the manufacturing, operation, management, processing, design, and development, handling, and delivery of products and services. This approach includes complete risk mapping and research of all layers of vendors' supply chains, the countries where products are manufactured and developed, where "reasonably" available. The policy also includes SCRM requirements for inclusion in contracts.

- **Software patches and updates must be scanned before being placed on production systems.** Best practice dictates that all patches and updates must be tested in a non-production environment to detect any flawed or malicious code before it has a chance to propagate throughout the HHS IT environment. A reasonable level of trust in vendors should be balanced against HHS's need to verify and validate the safety of software updates. Notwithstanding, because this event originated within third-party technology, HHS is enhancing processes to consistently work more closely with vendors to monitor potential security threats enterprise-wide. HHS notes, however, that in this case, the vendor notified HHS and took immediate action to remediate the cause of the compromise once detected.

- **A behavioral focus on cybersecurity is critical.** The SolarWinds exploit was detected after a leading cybersecurity firm observed anomalous network behavior. Employing technologies that focus on behavioral analytics and Zero Trust approaches to information access may help HHS identify threats before they are realized and limit the movement of attackers through the organization. HHS already requires users and devices to prove their identities before accessing the HHS network—a hallmark of Zero Trust.

Conclusion

HHS will continue taking every necessary precaution and action to address SolarWinds and other cybersecurity incidents in the future. We are mindful that our adversaries are already developing other cyber hacking approaches and capabilities. The Department with our partners remains vigilant, committed to addressing the unique and ever-changing challenges in cybersecurity to ensure all Americans' safety, security, and confidence in our digitally connected world.

Chairman Peters, Ranking Member Portman, and Members of the Committee, we appreciate the opportunity to testify today. I am happy to answer any questions you might have.

Thank you.