“Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign”
Committee on Oversight and Reform and Committee on Homeland Security Joint Remote Hearing
9:00 AM, Friday, February 26, 2021
Rep. Gerald E. Connolly (D-VA)

I thank Chairwoman Maloney and Chairman Thompson for holding this vital joint hearing today on the recent cybersecurity incidents affecting government and private sector networks, including the supply chain attack targeting SolarWinds Orion software.

On December 8, 2020, FireEye, a cybersecurity firm in the United States, reported that a suspected state actor, later identified as Russian in origin, had launched a successful cyberattack involving the company SolarWinds and its Orion software. FireEye uncovered that the attackers used a supply chain attack to compromise the development of SolarWinds’ Orion network monitoring software. This software is widely used throughout both private and public sectors.

On December 12, 2020, FireEye notified SolarWinds of the attack targeting its Orion product. On December 13, SolarWinds confirmed that malware had been inserted into its Orion software updates. On December 15, SolarWinds released the first of its software patches to remove the malicious code.

The bad actors in this supply chain attack reportedly accessed SolarWinds’ internal systems as early as September 2019, compromised the software development process for the Orion product, and between March and June 2020, placed Trojan horse malware called SUNBURST into software updates that were subsequently downloaded by SolarWinds’ customers.

Individuals in both the public and private sectors downloaded affected versions of the SolarWinds Orion software updates, exposing up to 18,000 customers to the malware. In addition, follow-on attack activity from the hacker has affected at least nine federal agencies, including the Departments of Health and Human Services, Homeland Security, State.

On January 6, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) announced that it was investigating instances of the attacker accessing systems through other means than the SolarWinds Orion compromise. In late January, the acting director of CISA stated that approximately 30% of victims had no direct connection to SolarWinds, making clear the complexity of the attack and the difficulty its victims would have understanding its processes and implications. For nine months, these bad actors had access to many private sector and federal government agency IT systems, with access to massive amounts of sensitive information.

The SolarWinds breach is the most significant espionage attack on our government systems in history. Its ramifications are amplified in the context of the coronavirus pandemic, which has made information technology (IT) a lynchpin of commerce and government and tested the capacities our federal IT systems. Further, this attack demonstrates the critical need to invest in and strengthen the federal government’s cybersecurity capabilities.

Information security is a critical component to all of the work being done in the federal government. While we will never be able to prevent all cyber-attacks, we can improve the federal government’s capability, readiness, and resilience in cyberspace. To mitigate the risk of cyber-attacks, we must work hand-in-hand with our private sector allies to patch vulnerabilities and facilitate clear communication.

The private sector plays a key role in our nation's cyber defenses, developing most of the essential information communications and technology products agencies rely on. In 2014, Congress passed the National Cybersecurity Protection Act, which formally designated the National Cybersecurity and Communications Integration Center as the portal for cybersecurity information-sharing and assistance between the public and private sector. In 2015, Congress passed additional legislation that enhanced threat information-sharing between the public and private sectors. This law, however, does not mandate private sector companies to report and share information about potential attacks with the federal government.

In January 2021, Congress passed the National Defense Authorization Act, which gave CISA the power to deploy technology, including information collection tools, on federal agency networks and applications and to conduct threat hunting excursions on those systems without notifying agencies in advance. It also calls for the Department of Homeland Security secretary to submit to Congress a review of CISA's ability to conduct such threat hunting given its resources within a year of enactment.

While this is an important first step in ensuring the federal government has the ability to mitigate cyber-attacks, more must be done.

A December 2020 Government Accountability Office report found that of the 23 civilian Chief Financial Officers Act agencies audited, *ZERO* had fully implemented the foundational practices for managing IT supply chain risks and 14 had not implemented any of the practices. The number one reason agencies cited for their limited implementation of the foundational practices was lack of federal guidance.

If we don't fix these glaring gaps, attacks will happen with regularity; we need to do better.

That is why I am fully supportive of the proposal and funding request of the IT modernization provisions in President Biden's American Rescue Plan, which would drastically improve the federal government's cybersecurity posture.

President Biden's proposal was not a one-and-done approach. It was a multi-pronged approach that included new funding, expanded authorities, and enhanced personnel. This approach would remediate the SolarWinds breach and would boost U.S. cybersecurity defenses overall. That kind of wholistic approach is a welcome perspective coming from the new Administration, and I look forward to working with them to make it a reality.

I want to thank these private sector witnesses for continuing to cooperate with both the Oversight and Reform Committee and Homeland Security Committee and I look forward to continuing to partner with the private sector on improving our cybersecurity posture by modernizing our IT systems and shoring up our supply chains.