CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

MEMORANDUM

February 23, 2021

To: Members of the Committee on Oversight and Reform

Fr: Majority Staff

Re: Joint Hearing on "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign"

On **Friday, February 26, 2021, at 9:00 a.m., via the WebEx video platform**, the Committee on Oversight and Reform and the Committee on Homeland Security will hold a joint remote hearing on recent cybersecurity incidents affecting government and private sector networks.

I. BACKGROUND AND PURPOSE

In December, the U.S.-based cybersecurity firm FireEye reported that a suspected state actor, later identified as likely Russian in origin, had launched a successful cyberattack involving the company SolarWinds and its Orion software.[1] FireEye uncovered that the attacker used a "supply chain attack" to compromise the development SolarWinds' Orion network monitoring software, which is widely deployed throughout the private and public sectors and requires high levels of access on customer networks to perform its functions.[2]

The attacker in this supply chain attack reportedly accessed SolarWinds' internal systems, compromised the software development process for the Orion product, and placed Trojan horse malware into software updates that were subsequently downloaded by SolarWinds'

---

[1] FireEye, *FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community* (Dec. 8, 2020) (online at www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html); FireEye, *Global Intrusion Campaign Leverages Software Supply Chain Compromise* (Dec. 13, 2020) (online at www.fireeye.com/blog/products-and-services/2020/12/global-intrusion-campaign-leverages-software-supply-chain-compromise.html).

[2] *Hackers Used SolarWinds' Dominance Against It in Sprawling Spy Campaign*, Reuters (Dec. 15, 2020) (online at www.reuters.com/article/idUSKBN28P2N8); *Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit*, New York Times (Dec. 14, 2020) (online at www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html).

customers.[3] According to the company, nearly 18,000 customers downloaded the malicious software update between March and June 2020.[4] After the malicious update was installed, the attackers received information about the host systems and could select targets for further attacks. Once inside a victim's network, the attackers moved stealthily, escalated privileges, and accessed data, including e-mails.[5] To date, follow-on attack activity has affected nine federal agencies and approximately 100 private sector companies, and may still be ongoing.[6]

The hearing will examine the supply chain attack targeting SolarWinds Orion software and other cyberattacks, the role of the private sector in preventing, investigating, and remediating these attacks, and public-private coordination.

II. WITNESSES

Sudhakar Ramakrishna (providing opening statement and answering questions)
President and Chief Executive Officer
SolarWinds Corporation

Kevin B. Thompson (not providing opening statement, but answering questions)
Former Chief Executive Officer
SolarWinds Corporation

Kevin Mandia
Chief Executive Officer
FireEye, Inc.

Brad Smith
President and Chief Legal Officer
Microsoft Corporation

Staff contacts: Peter Kenny, Greta Gao, Courtney French, and Gina Kim at (202) 225-5051.

---

[3] Cybersecurity and Infrastructure Security Agency, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations* (Dec. 17, 2020) (online at https://us-cert.cisa.gov/ncas/alerts/aa20-352a).

[4] SolarWinds Corporation, *FAQ: Security Advisory* (updated Feb. 5, 2021) (online at www.solarwinds.com/sa-overview/securityadvisory/faq).

[5] Microsoft Corporation, *Using Microsoft 365 Defender to Protect Against Solorigate* (Dec. 28, 2020) (online at www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/).

[6] The White House, *Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger* (Feb. 17, 2021) (online at www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/).