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

Opening Statement
Chairwoman Carolyn B. Maloney
Committee on Oversight and Reform
Hearing on "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and Ongoing Campaign"
February 26, 2021

Good morning. I want to welcome everyone to this joint hearing of the Committee on Oversight and Reform and the Committee on Homeland Security. Welcome to Chairman Thompson, Ranking Member Katko, Ranking Member Comer, and all of our Members.

Today's hearing is the first in the House on the cyberattack uncovered last year that initially targeted the software company SolarWinds and its Orion product. The details are truly frightening.

Here is what we know: a sophisticated attacker—reported to be the Russian government—broke into SolarWinds' systems and inserted malicious code into its software, which customers then downloaded. The numbers tell how dangerous an attack like this can be—nearly 18,000 customers downloaded updates containing the malicious code.

It's not just the number of potential victims—as staggering as that is—or even the number of known victims of secondary attacks, but the nature of this attack and the profiles of victims that should give us all grave concern.

Among the victims were major technology companies—some of which have the best cybersecurity in the world—as well as critical infrastructure firms, our nation's law enforcement, and government agencies involved in foreign affairs and national security.

It has affected approximately 100 private sector companies and at least nine federal agencies, including the Departments of Homeland Security, Justice, State, and Treasury.

And that's just what we know. There is much more that we still don't know, including one of the most critical questions: are they still inside? In the weeks and months ahead, our Committees will continue our joint investigation to examine other aspects of this massive attack.

Today, our focus is on the private sector. The private sector plays a key role in our nation's cyber defenses. They own critical infrastructure, and they develop essential information communications and technology products. They help the government and other companies secure and defend their own networks.

It was the private sector that uncovered this attack—not our own government. Specifically, FireEye discovered it, reported its findings, and shared it with the world. Had FireEye not taken that action, the attack could very well be fully up-and-running today.

At the same time, the private sector was targeted as part of a campaign to gain access to government networks and other entities. All of the companies here today are victims of this attack, and all provide products and services to the government. That puts the government at risk.

Additionally, it is the private sector to whom the government must turn. In particular, the government has turned to Microsoft to learn whether it was exposed and how badly due to the widespread adoption of Office365 Cloud.

The private sector must be held accountable for its role. Our Committees recently obtained a presentation made by a former employee at SolarWinds named Ian Thornton Trump. The 23-page presentation, appears to include a proposal from 2017 that stated, "The survival of the company depends on an internal commitment to security. The survival of our customers depends on a commitment to build secure solutions." I look forward to hearing from Mr. Thompson about the steps the company took in response.

Cybersecurity demands strong leadership, but unfortunately, we've suffered under four years of terrible leadership at the very top. On December 18, Secretary of State Mike Pompeo stated during a public interview, quote: "This was a very significant effort, and I think it's the case that now we can say pretty clearly that it was the Russians that engaged in this activity." Yet, the very next day, President Trump tweeted this, and I quote: "The Cyber Hack is far greater in the Fake News Media than in actuality."

So, what can we do now? First, I'm pleased that the Biden Administration has taken early steps to elevate the importance of cybersecurity and supply chain risk. Our Committee plans to focus on federal procurement—the government pays hundreds of billions of dollars for goods and services each year. We must demand better cybersecurity practices from our suppliers, as well as increased information-sharing with the private sector. Finally, the Oversight Committee plans to closely review agency roles, responsibilities, and strategy under the Federal Information Security Modernization Act—known as FISMA—to meet the complex and dynamic cybersecurity landscape of today.

Much work needs to be done. Today—and in the weeks and months ahead—we will focus on the facts, with an eye towards legislative solutions and how we can improve cyber-defenses across both the public and private sectors.

###

Contact: Aryele Bradford, Communications Director, (202) 226-5181