U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Opening Statement

Chairman Bill Foster (D-IL)
of the Subcommittee on Investigations and Oversight

Joint Hearing of the
Investigations & Oversight and Research & Technology Subcommittees:
SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains
May 25, 2021

Good morning, and welcome to our members and panelists. Thank you for joining us for this important hearing on supply chain cybersecurity. We're focusing on the software supply chain today. And cybersecurity attacks through the software supply chain are a special kind of insidious. Supply chain attacks are harder to detect, to prevent, and to remediate than traditional malware.

And once an adversary is in the system, they can deploy multiple types of attacks to maintain access and steal data. They might run amok on your system for a long time once they're in, because their access came through a trusted partner. In the case of SolarWinds, the Russian intelligence service embedded a backdoor in the company's Orion software in the fall of 2019. Customers were downloading the infected software by the spring. 18,000 organizations did this over the course of 2020. And not one of them realized that they had company on their networks until FireEye detected the breach on their own systems and sounded the alarm in December.

I want to thank FireEye for moving quickly to alert public officials to what it had discovered. This is an esteemed cybersecurity company that was itself breached by a malicious actor. They might have worried about how news of the hack could affect the company's reputation, but did the right thing anyway. And we have since woken up to the fact that FireEye could have just as easily kept quiet, because there is no requirement for private companies to disclose a cybersecurity breach to the Federal government.

If a reputable cybersecurity company like FireEye can be breached by an attack like this, any organization can. And as we will hear from our Atlantic Council witness, Dr. Herr, supply chain cyber attacks are ticking up. In fact, we've seen several alarming incidents reported even since the SolarWinds breach was discovered in December.

And I have concerns about whether Federal agencies are doing enough to reduce their exposure to cyber risks, and whether they have systems in place to respond quickly to a breach. Last summer, Microsoft discovered a serious vulnerability called Zerologon that made it possible for the hackers to impersonate any computer on a network, including the system designed to identify and authenticate trusted people on the network. Microsoft issued the first of two patches on August 11. But by late September, some Federal agencies had still failed to update their systems.

The DHS Cybersecurity office, CISA, had to issue an emergency order to force agencies to patch or disable affected Windows servers. Meanwhile, it was discovered that the breach was already being exploited in the wild by Iranian and Russian hackers.

Malicious actors with a creative flair for exploiting technology are working every day to put Americans at risk. But the engineers at NIST and other Federal agencies are innovating, too. President Biden has released an Executive Order on improving Federal cybersecurity that calls on agencies to take bold actions to address the challenge of software supply chain security. I look forward to hearing today about how the Federal science apparatus can do more to understand the threat and help the private and public sectors mitigate their risk.

I'm also glad to partner with Ranking Member Obernolte on this important matter. I believe he is the first and only Member of Congress with an advanced degree in artificial intelligence. I'll ask him to put his technology executive hat back on today to help us get to the heart of the matter. I thank him and his staff for their partnership, and I yield for his opening statement.