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

Opening Statement

Chairwoman Haley Stevens (D-MI)
of the Subcommittee on Research and Technology

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 this joint hearing of the Subcommittee on Research and Technology and the Subcommittee on Investigations and Oversight. I would like to thank my esteemed colleagues, Chairman Foster and Ranking Member Obernolte, for leading this joint hearing. As the SolarWinds incident revealed, software supply chain issues are a threat to our Federal agencies and businesses across the country, including my district in Michigan.

This hearing comes at an auspicious time. President Biden's recent Executive Order "Improving the Nation's Cybersecurity" represents what I hope to be a sea change in how the Federal government approaches cybersecurity, from modernizing Federal IT systems to strengthening how the government responds to cyber threats from our adversaries.

The Executive Order focuses heavily on software supply chain issues, the topic of this hearing. It seeks to help software developers identity vulnerabilities before they release their software and help consumers better understand the security of the products they buy.

It should not be a surprise that I am excited to have NIST represented on this panel to talk about their leadership in cybersecurity standards and best practices.

NIST has a big role to play in the implementation of the Executive Order. The agency must develop broad standards for the security of the software supply chain within 90 days. Within 60 days, the agency must also identify and define what constitutes "critical software" and create special standards to protect it. Also within 60 days, NIST must develop standards so that software developers can test their source code. These timelines are aggressive, and I only mentioned some of the things that NIST is being asked to do.

NIST is highly respected for its role in incorporating input from its private and public sector partners to develop effective cybersecurity standards. But this work takes time and resources. NIST's entire cybersecurity and privacy portfolio was funded at only $78 million in last year's budget. I worry that we are increasingly asking NIST's experts to do exponentially more work, more quickly, with inadequate resources.

Moreover, GAO has found that Federal agencies are not adopting the guidance already on the books to deal with software supply chain threats. Additional guidance may be necessary, but we must also ensure agencies prioritize implementation of the guidance that already exists, and provide adequate resources for them to do so.

Congress and the Biden Administration must think creatively about modernizing the Federal government's approach to cybersecurity. I welcome the recommendations of this expert panel on how we can ensure that cybersecurity guidance developed as part of the Executive Order is operational, effective, and relatively easy to adopt.

I want to again thank the witnesses for being here today to help us tackle these challenging issues. I yield back.