COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
REPUBLICANS Frank Lucas, Ranking Member

Opening Statement of Ranking Member Michael Waltz

Joint Investigations & Oversight and Research & Technology Subcommittee Hearing

"SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains"

May 25, 2021

Thank you, Chairman Foster and Chairwoman Stevens for holding today's joint subcommittee hearing.

I also want to thank our distinguished panel of witnesses for their participation today. I am looking forward to hearing your expert testimony. I hope we will use this opportunity to learn more about software supply chain attacks and their impacts on federal agencies and examine how to improve our nation's software supply chain security. The Committee on Science, Space, and Technology has held several hearings over the years on bolstering the federal government's cybersecurity, and I am pleased to see that the Committee is still playing an active role in enhancing our nation's cybersecurity posture.

The recent SolarWinds, Microsoft Exchange, and Colonial Pipeline incidents make it clear that the United States is continuously being targeted with malicious cyber-attacks by nation-states and criminal actors. China, Russia, Iran, and other malign actors are focusing on cyber capabilities. Unfortunately, these attacks are not the first, and certainly will not be the last of their kind.

The National Institute of Standards and Technology (NIST) is the primary federal agency responsible for setting standards and guidelines for federal agencies and provides voluntary best practices for private industry. In 2014, NIST published a voluntary risk-based Cybersecurity Framework with a set of industry standards and best practices to help organizations manage cybersecurity risks. Additionally, NIST has established guidance specifically related to supply chain security, including the Cyber Supply Chain Risk Management (C-SCRM) framework and the Secure Software Development Framework (SSDF) to help identify, assess, and mitigate supply chain risks.

On May 12, 2021, the President issued an Executive Order (EO) on Improving the Nation's Cybersecurity, which entrusts multiple federal agencies, including NIST, with strengthening the security of the software supply chain. Section 4 of the EO directs the

Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security.

Based on my experience in the National Guard, I would like to see NIST consult with the cyber talent within the Guard when executing Section 4 of the EO. The National Guard and Reserve retains elite cyber talent from both Silicon Valley and the Pentagon and can effectively serve as a bridge between the private sector and federal government. This EO is a good starting point for addressing vulnerabilities in our nation's software supply chain, but there is more work to be done.

A recent Government Accountability Office (GAO) report assessed federal information and communications (ICT) supply chain risk management (SCRM) practices and the findings are alarming. None of the federal agencies reviewed had fully implemented the SCRM practices, and approximately 60 percent of these agencies had not implemented any of the practices. As a result, GAO identifies 145 recommendations for agencies to fully implement foundational practices in their approach to ICT SCRM.

Moving forward, we must work diligently to provide agencies with the resources to move swiftly to close the gap between recommendations and implementation of foundational practices. Cybersecurity frameworks are otherwise useless unless proper funding and support are available to fully implement them.

Additionally, NSF's CyberCorps: Scholarship for Service program should receive consideration by the committee for enhancing the federal government's cybersecurity workforce.

Time is of the essence, and it is imperative that modernized cyber defenses are implemented to get ahead of the next cyber-attack from China, Russia, Iran and other adversaries. We cannot afford to let foreign adversaries and cyber criminals take advantage of weaknesses in software supply chains as the consequences can be detrimental to the national and economic security of the United States.

Thank you, and I yield back.