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

Opening Statement as Prepared for Delivery of Ranking Member Jay Obernolte

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 hearing on improving the cybersecurity of software supply chains. And thank you to the panel of expert witnesses for taking time to help educate us on this very timely and important topic.

Recent cyber incidents like SolarWinds, Microsoft Exchange, and Colonial Pipeline have thrust the issue of cybersecurity into the limelight. The most notorious and perhaps the most pernicious of these incidents is SolarWinds – a software supply chain attack that impacted roughly 100 organizations and at least 9 Federal agencies.

Although analysis and investigation into this incident is ongoing, the details that have emerged thus far paint a troubling picture for the state of Federal cybersecurity.

Advanced cyber actors infiltrated SolarWinds' build environment, surreptitiously implanted malicious code into a an otherwise valid software update, and then waited for that update to be downloaded. Ultimately, the actors responsible for this software supply chain attack abused the trusted relationship that SolarWinds had with its customers—including federal entities—by compromising the software update with a "backdoor" that could be leveraged against the actors' intended targets, like the 9 federal agencies impacted by this incident. The update was then made available for download by SolarWinds' customers, with no indication to them that the update had been tainted by cyber adversaries.

The amount of time that this actor was able to lie dormant, undetected in federal networks is particularly concerning – it took almost two years before Federal agencies discovered the intrusion. And only then with the help of the cybersecurity firm FireEye. The SolarWinds incident makes clear that the Federal government must do more to secure its software supply chains.

In December 2020, GAO published a report based on its investigation into federal agency implementation of Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) foundational practices. The findings are disturbing.

GAO found that none of the federal agencies it reviewed had fully implemented foundational practices for ICT SCRM, and that roughly 60% of the agencies reviewed had not implemented any of the foundational ICT SCRM practices. This is unacceptable.

In May, the Biden Administration signed Executive Order 14028 on improving the nation's cybersecurity. The EO, among other things, tasks NIST with identifying existing or developing new guidance to help improve the security of software supply chains.

While this is a step in the right direction, proper implementation is critical to its success. For example, NIST has several products to inform Federal agency ICT SCRM practices. In fact, the GAO report I referenced earlier derived its seven foundational ICT SCRM practices from NIST guidance. Nevertheless, the reason most frequently cited by agencies for their failure to implement identified practices was a lack of clear Federal guidance. Without proper implementation by Federal agencies, more guidance, best practices, and other resources will be useless.

To that end, we need to find a better way to conduct oversight of agencies' implementation of this guidance, and agencies must be more accountable for their responsibilities under FISMA to secure the information and systems for which they are responsible.

I look forward to learning more from our witnesses today about how we can get agencies the implementable guidance that they need to shore up the security of their software supply chains, and the resources needed to see implementation is carried out across the board.

Thank you to our panelists for being here today. And thank you again to Chairman Foster and Chairwoman Stevens for holding this important hearing. I yield back the balance of my time.