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

**Chairwoman Eddie Bernice Johnson (D-TX)**

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

Good afternoon to our witnesses and thank you for joining us here today.

Securing Federal government systems from cyberattack is an evolving challenge. We have repeatedly seen the importance of getting it right, and the painful consequences of getting it wrong. As SolarWinds and other recent attacks have shown, the software supply chain is especially challenging to protect. We must ensure that the Federal Government is coordinating effectively to secure our IT systems.

Jurisdiction over cybersecurity is widely shared across Congressional committees and Federal agencies. I want to affirm the Science Committee's role on cybersecurity matters. The scope of jurisdiction for authorizing committees in the technology space was last changed significantly in 2002. That's when Congress created the House Homeland Security Committee and the Department of Homeland Security in response to 9/11.

That same year, Congress passed the Federal Information Security Management Act, or FISMA. FISMA was updated in 2014 and became the Federal Information Security Modernization Act. FISMA called on Federal agencies to develop information security programs to protect themselves. The Science Committee focus is on developing tools for prevention. Specifically, we are responsible for directing and overseeing the National Institute of Standards and Technology's role in cybersecurity. Under FISMA, NIST creates cybersecurity standards and guidance for the government. The Science Committee is one of the three House Committees that receives cyber incident reports under FISMA.

It's hard to comprehend how much the cybersecurity landscape has changed since 2002. The threats that Federal agencies and the private sector face today are sophisticated and relentless. Recent attacks have shown that existing oversight mechanisms are not enough. After the SolarWinds attack was revealed, information was slow to emerge. Briefings and reports to Congress were unpredictable in their timing and their content. Federal agencies reported that they were not able to share information with other agencies. Determinations of whether the incident was reportable to Congress or not were based on a one-size-fits-all form. I worry we are not capturing the full extent of the potential harm from attacks on our Federal systems.

We must do better, both in mitigating attacks after they happen and in preventing them in the first place.

This has been and will continue to be a bipartisan concern on this Committee. I look forward to continuing to work with Ranking Member Lucas and our colleagues on the Committee to reinforce NIST's role in cybersecurity.

There is simply so much work to be done on cybersecurity – both for policymakers and for practitioners in the field. I am glad that the witnesses here today offer a wide range of expertise to help us chart our next steps.

Thank you, and I yield back.