Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
March 18, 2021

I want to thank our witnesses for joining us today and for their service to the American people. This hearing will examine the devastating impact of recent cyber-attacks against our federal networks, including the dire national security implications of last year's SolarWinds breach and other recent online espionage efforts.

This was one of the most destructive cyber breaches in American history, and there are still many unanswered questions about how it happened, and how it went undetected for so long.

Both the SolarWinds and recent Microsoft hacks clearly show that our nation is not adequately prepared to tackle this persistent and grave threat.

Foreign adversaries, like China and Russia, continue to exploit our cyber vulnerabilities to access confidential and classified information, disrupt government operations, and even target businesses, schools and critical infrastructure. Unless our capabilities are able to match the threats we face, American networks and supply chains remain at risk.

Last year's SolarWinds hack and the subsequent breach of federal systems was incredibly sophisticated and the extent of the damage is astounding. We must prevent an espionage effort like this from ever happening again, and ensure our government has the resources to calibrate our response to these threats.

After the SolarWinds hack, likely perpetrated by the Russian government, our agencies were asked to self-analyze and review the effects of the attack when many did not have the capabilities to do so. This haphazard approach made it extremely clear our ability to respond did not match the severity of the crisis.

The process and procedures for responding to cyber-attacks desperately needs to be modernized, including improving the *Federal Information Security Modernization Act*, which has not been updated since the creation of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.

In order to adapt to the evolving cybersecurity threat, both the public and private sector need a centralized, transparent, and streamlined process for sharing information. In the event of a future attacks, this will be critical to mitigating the damage.

This discussion, with our government's foremost cyber experts, will be critical to understanding how agencies are assessing the damage done by these breaches and what action they took to notify Congress.

Going forward, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency will play a critical role in strengthening our cyber defenses and the security of our federal systems and supply chains.

Mr. DeRusha, as the Federal Chief Information Security Officer, you are charged with implementing and coordinating these efforts. Based on your strong record in my home state of Michigan and your extensive experience, I have every confidence you are up to the task.
I have long raised concerns about the national security threat posed by cyber-attacks, but those challenges continue to grow. The pandemic has pushed much our lives and communities online, and foreign adversaries and other bad actors continue to target the networks of our research institutions and health systems, threatening our ongoing pandemic response.

That is precisely why, as a part of *the American Rescue Plan Act*, I helped secure nearly $2 billion to update our aging federal information technology systems and help address cybersecurity threats. However, it is clear from the gravity of this threat, we need to examine whether CISA, the FBI and other agencies have what they need to protect the American people.

I am committed to working on a bipartisan basis with my colleagues on the committee, especially Ranking Member Portman, and with the Biden Administration, to protect our networks against future breaches. This hearing is the first of several that we will hold on this issue. We must tackle this problem both swiftly and comprehensively.