OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
PREVENTION, RESPONSE, AND RECOVERY: IMPROVING FEDERAL CYBERSECURITY POST-SOLARWINDS

May 11, 2021

Thank you, Chairman Peters. I've appreciated our bipartisan work over the years to improve federal cybersecurity and I look forward to continuing our partnership.

We are here today to continue our oversight of the massive SolarWinds hack and other recent cyberattacks, analyze their impact on specific federal agencies, and discuss how we can learn from these incidents to improve our cyber defenses in the future. As many of you know, we are in the process of writing legislation to address these issues. This is our second hearing to discuss this important topic and I look forward to hearing the perspective of the agency officials on the ground fending off these cyberattacks.

In the last six months, hackers executed four known major cyber campaigns against U.S. government agencies and private companies—SolarWinds, Microsoft Exchange, Pulse Secure, and most recently, Colonial Pipeline. The SolarWinds and Pulse Secure VPN attacks targeted federal agencies, yet it was private sector companies that discovered these intrusions. Despite all the increased funding appropriated for cybersecurity and the bipartisan legislation we've worked on here in this committee, **not one** of these federal intrusions was discovered by the federal government. This should be concerning to all of us here. Cyberattacks will continue to be a threat and the federal government needs to be able to identify them and defend itself.

We continue to learn about these attacks. Here are some details we know already:

- **First, since our last hearing, the U.S. government officially attributed the SolarWinds hack to Russia's foreign intelligence service, or the SVR.**

- SVR was patient about selecting its targets and compromised a trusted link in the software supply chain.

- It disguised its activity and used stealth techniques that evaded detection.

- Because of that, it took more than a year to detect the attack—a lifetime to do damage for sophisticated adversaries like these.

- **Second, we know the SolarWinds and Microsoft Exchange attacks were broad.**

  - Within the federal government, the SolarWinds attack hit agencies holding some of our most sensitive data and national security secrets—including the agencies here today.

  - I look forward to the testimony of our witnesses about the impacts of recent attacks on their agencies.

  - The SolarWinds and Microsoft Exchange attacks also impacted the private sector, even cybersecurity firms.

  - For example, FireEye, the company who discovered the SolarWinds hack, was breached. FireEye is one of the firms folks call when they discover a breach. So, here, the very people we call when we get hacked, got hacked themselves.

  - We are still in the very early stages of learning about the Pulse Secure attack, but recent reports indicate at least five federal agencies were compromised.

- **Third, the fact the federal government was hacked is not surprising.**

  - In June 2019, as then Chairman of the Permanent Subcommittee on Investigations, I released a report with Senator Carper detailing the extensive cybersecurity

vulnerabilities of eight federal agencies. Many of these vulnerabilities had remained unresolved for a decade.

- More than a year later, three of those agencies were seriously compromised by the SolarWinds attack: DHS, State, and HHS.

- State is not here but HHS is here and we will look forward to a dialogue about why HHS did not declare a major incident under the Federal Information Security Modernization Act, or FISMA.

- I am deeply concerned that members of DHS's cybersecurity team who hunt threats from foreign countries and the former DHS Secretary were compromised in the SolarWinds attack and that we learned about this from news reports. Mr. Wales, I look forward to a discussion of how CISA specifically, which is a part of DHS, was impacted.

- **Finally, it's clear that cyberattacks are going to keep coming.**

  - Last week, cyber criminals attacked Colonial Pipeline, the company responsible for providing 45% of the East Coast's fuel.

  - This is potentially the most substantial and damaging attack on U.S. critical infrastructure to date.

  - It shows that cyberattacks can have tangible, real-world consequences.

  - Although our witnesses today are here to discuss federal cybersecurity, I think it is important that we hear from CISA about what we know so far about this attack and what we should be doing to deter, detect, and respond to attacks like this in the future.

- **These four recent attacks have demonstrated not only the weakness of our defenses, but also the persistence and sophistication of our adversaries.**

In response, we have to take a hard look at our federal cybersecurity strategy, capabilities, and leadership and discuss what changes are necessary to prevent and mitigate attacks like this in the future.

At our last hearing, I asked our witnesses who is ultimately accountable for federal cybersecurity. The witnesses were not able to give me a clear answer, which is troubling.

- Under current law, each agency is ultimately responsible for securing its own networks, which is why we asked agency Chief Information Security Officers, or CISOs, to give their perspective today.

- But, CISA must also have visibility across federal civilian agencies to be able to do what Congress created it to do: secure the networks of the federal government.

- Congress also created the position of the National Cyber Director in the White House to coordinate implementation of national cyber policy and strategy, as recommended by the Solarium Commission. The Biden Administration has now nominated Chris Inglis and I understand his paperwork is being finalized.

- It appears that the Deputy National Security Advisor for Cyber and Emerging Technology, Anne Neuberger, has also taken a leading role in handling cyberattacks.

- I believe a single point of accountability for federal cybersecurity overseeing all of this—the individual agency efforts and CISA's work to support them—is crucial.

I appreciate the witnesses being here today, and look forward to your testimony on these important issues.

Thank you.