OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
UNDERSTANDING AND RESPONDING TO THE SOLARWINDS SUPPLY CHAIN ATTACK: THE FEDERAL PERSPECTIVE

March 18, 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 this Congress.

We are here today to understand more about the massive SolarWinds hack, analyze its impact on the federal government, and discuss what changes are necessary to prevent and mitigate attacks like these in the future.

It has been three months since we learned of the attack and there is still a lot that remains unknown. But what we *do* know is chilling:

- **First, according to the FBI, the attackers were "likely Russian in origin."** [1] **They were also smart and hard to detect.**
    - They were patient, and careful about selecting their targets.
    - They disguised their activity and used stealth techniques that evaded detection.
    - And because of that, it took over a year to detect the attack—a lifetime to do damage for sophisticated adversaries like these.
- **Second, we know the attackers used a trusted software company, a supplier to attack the U.S. government**.
    - The attack compromised a security update or "patch" for the widely used SolarWinds Orion IT management software.

[1] FBI, CISA, ODNI, & NSA Joint Public Statement (Jan. 5, 2021), https://www.cisa.gov/news/2021/01/05/joint- statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

- We all know that good cybersecurity practices include applying updates and security "patches" in software.

- Here, the attacker used a security patch meant to better protect against hacks to launch the attack. The attacker capitalized on our assumption that these patches are safe to install.

- This should be a wakeup call for all of us who are concerned about our data being compromised.

- **Third, we know that this attack was broad—both the federal government and private sector were impacted.**

  - Within the federal government, this attack hit agencies that hold some of our most sensitive data and national security secrets. Based on public sources, this includes the State Department, the Department of Homeland Security, the National Institutes of Health, and the National Nuclear Security Administration—the agency charged with maintaining our nuclear stockpile.

  - The SolarWinds attack also impacted the private sector, even cybersecurity firms like FireEye, who discovered the breach in its own systems.

  - To be clear, FireEye is one of the firms folks call when they discover a breach. So, here, the very people we call when we get hacked, themselves got hacked.

- **Fourth, we know that despite all the increased funding that has been appropriated for cybersecurity, the federal government never caught this attack.**

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.

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

- And those are just the three we know of today.

The SolarWinds attack was one of the most widespread and consequential cyberattacks to date. In response, we have to take a hard look at our federal cybersecurity strategy and defense capabilities.

- This includes the failure of the federal government's front-line defense program called EINSTEIN.

- EINSTEIN has cost approximately $6 billion and is supposed to detect and prevent cyber intrusions at federal agencies.

- Clearly, it was ***not*** effective in stopping the SolarWinds breach.

- EINSTEIN's authorization expires at the end of next year, so it is a good time to consider its utility.

Any cybersecurity legislation we consider needs to address the broad set of risks facing federal networks, and needs to ensure there is proper expertise and accountability in the U.S. government. When those networks are breached, as in the case of SolarWinds, there must be consequences.

I appreciate the witnesses being here today, and look forward to your testimony on these important questions and your ideas on how we can better defend our federal networks.

Thank you.