Chairman Peters Opening Statement As Prepared for Delivery
Full Committee Hearing: National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems
September 23, 2021

I want to thank our witnesses for joining us today and for their service to the American people. Your agencies and offices are vital to protecting federal cyber networks and critical infrastructure systems.

Although it can often be difficult to understand the complexity and severity of many cyber-attacks, they are only increasing in sophistication and frequency, and have a significant cost on our national security.

The Federal Bureau of Investigation reported 2,474 ransomware attacks in 2020, though experts believe the actual number is much, much higher.

Just last month, in my home state of Michigan, about 1,500 patients were notified that their information had been exposed as a result of the breach of a file-sharing service used by their hospital.

This breach, like the SolarWinds attack, is yet another example of how our adversaries will target vendors and contractors, including small businesses, to find the weakest link, and exploit our greatest vulnerabilities.

In order to prevent these types of attacks, potential victims, from the public sector to the private sector, must be aware of these ever-changing threats, and have the right information to safeguard their networks.

Whether it's widespread spyware, or a ransomware attack, the federal government needs to know when cyber incidents have occurred, so they can determine if there are patterns, alert future potential targets, and help seal up any vulnerabilities.

This information is especially vital when it comes to our nation's critical infrastructure, 85% of which is privately owned and operated.

Despite this vulnerability there is currently no national requirement for all critical infrastructure owners and operators to report to the federal government when they have been hit with a significant attack. That needs to change.

As we have seen from recent attacks on an oil pipeline, water treatment plants, food processing facilities, and hospitals, these breaches can cause serious economic and national security concerns, and disrupt our daily lives.

If multiple critical infrastructure entities, like energy companies for example, are reporting similar attacks, then CISA and other federal entities should be able to warn others, prepare for potential impacts to that sector or other related sectors, and help prevent further widespread attacks.

Ranking Member Portman and I are currently working legislation that we plan to introduce soon, to require critical infrastructure companies that experience cyber incidents, and other entities that make ransomware payments, to report this information to CISA.

This requirement will ensure CISA and other federal officials have better situational awareness of ongoing cybersecurity threats, who the targets are, how the adversary is operating, and how best to protect the nation.

I'm looking forward to hearing from our witnesses today about how an incident reporting law could help each of your organizations assist victims in recovering from an attack and prevent them from happening in the first place.

But we also need to ensure the federal government is sharing this same information in a timely manner.

The last time Congress substantially addressed federal cybersecurity was in 2014, when this Committee, led by then Chairman Carper, passed the *Federal Information Security Modernization Act*.

Since then, our technology has developed rapidly, along with the sophisticated threats we face. When that legislation was passed, CISA had not yet been created.

We need to pass updated legislation that clarifies CISA's roles and responsibilities in federal information security, improves how incidents on federal networks are reported to Congress, and ensures that our cybersecurity resources are effectively aligned with emerging threats. Ranking Member Portman and I are also working on legislation that would help achieve these goals.

We also need a better understanding of how the federal government is balancing its responsibility to bring cybercriminals to justice and helping victims recover from an attack.

We learned earlier this week that in one instance, the FBI withheld a digital key that could have aided victims for several weeks to pursue its investigation.

In order to conduct thorough oversight, this Committee needs to know more about the federal government's processes for assisting the victims of attacks, and how your agencies weigh investigative, national security, and economic needs.

Finally, I want to acknowledge the important actions the Biden Administration has already taken to bolster our cybersecurity defenses, improve information sharing, and apply the lessons learned from previous breaches to avoid future attacks. The President's Executive Order "On Improving the Nation's Cybersecurity," for example, is paramount to securing our nation.

This is a top priority for both myself and Ranking Member Portman; and I look forward to today's discussion and working productively with these vital federal agencies to ensure we are addressing this harmful threat.