OPENING STATEMENT
RANKING MEMBER ROB PORTMAN
NATIONAL CYBERSECURITY STRATEGY: PROTECTION OF FEDERAL AND CRITICAL INFRASTRUCTURE SYSTEMS

September 23, 2021

Thank you, Chairman Peters for convening this hearing to continue our bipartisan oversight of Federal cybersecurity.

We are here today to discuss the Federal Government's strategy for protecting our cyber networks and critical infrastructure. One important part of that strategy is accountability and I hope to have a conversation about the appropriate roles and responsibilities for the many different cybersecurity positions within the Federal Government. I also look forward to discussing how cyber incident reporting legislation might better inform that strategy.

In recent years, hostile cyber adversaries, both foreign and domestic, have executed some of the most damaging cyberattacks in our history. Both the Federal Government and private sector companies have been targeted. We held hearings on several of these incidents here in this Committee—including the SolarWinds and Colonial Pipeline attacks. Both of these events are stark reminders of the wide-ranging and real world impacts of sophisticated cyberattacks.

As these attacks become more and more common, it is important that we work to protect ourselves and our networks. We know that one of the best strategies for preventing these attacks is to improve baseline cybersecurity practices. We also know that Federal agencies have failed to make meaningful progress on the implementation of these practices as required by the Federal Information Security Modernization Act or FISMA.

In August, just last month, Chairman Peters and I released a report detailing the significant cybersecurity vulnerabilities of eight key Federal agencies—the Departments of Homeland Security, State, Transportation, Housing and Urban Development, Health and Human Services, Agriculture, and Education, and the Social Security Administration. This report follows a 2019 report I released with Senator Carper as Chairman of the Permanent Subcommittee on Investigations evaluating the same eight agencies.

In this year's report, only DHS had an effective cybersecurity program. Every other agency featured in the report failed to meet this standard. We also found the average grade across all Government agencies was a C minus. The report identifies several common agency vulnerabilities including the failure to: (1) adequately protect personally identifiable information; (2) maintain an accurate and up to date list of the agency's IT assets; (3) install security patches in a timely fashion; and (4) retire vulnerable legacy technology that is no longer secure.

Securing fragmented networks against increasingly sophisticated attackers is not a trivial task. It would be unfair to suggest otherwise. Yet, in the nearly seven years since FISMA was last updated in 2014, agencies still have the same vulnerabilities year after year.

Accountability is a crucial aspect of any strategy. All three witnesses with us here today have heard me discuss the importance of it for Federal cybersecurity in particular. Without appropriate accountability for Federal networks and agency systems, among the three of you and the Deputy National Security Advisor for Cyber, I believe that we will continue to see these consistent and long-standing vulnerabilities. We need to be clear about who is in charge to better prevent and respond to cyber attacks. I hope we can continue the discussion of how we can best achieve that accountability here today.

We are also here to discuss another important topic in the development of an overarching strategy: cyber incident reporting. Recent attacks on critical infrastructure, particularly through ransomware, demonstrate how prompt notification to the government can benefit both the government and victims. In the case of the Colonial Pipeline attack, the FBI was able to recover part of the ransom paid by Colonial to the attackers. There is a balance between getting information quickly, letting victims respond to an attack without imposing onerous requirements on them, and getting accurate information. I look forward to the witnesses' perspectives on how to balance these competing priorities.

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