

Opening Remarks
Ranking Member Rob Portman
Business Meeting
Homeland Security and Governmental Affairs Committee
October 6, 2021

Thank you, Chairman Peters. I appreciate everyone coming together this morning.

Today, we have two important cybersecurity bills to consider. 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. We need greater transparency into the frequency and effect of these attacks.

The Cyber Incident Reporting Act will require critical infrastructure to report to DHS—through the Cybersecurity and Infrastructure Security Agency or CISA—within 72 hours when a breach occurs. All entities except individuals and small organizations will also provide notice of ransomware payments within 24 hours. This information should give CISA, and its federal law enforcement partners, greater insight into cyber attacks on critical infrastructure to better combat this threat.

We also know that Federal agencies have failed to make meaningful progress on the implementation of strong cybersecurity practices as required by the Federal Information Security Modernization Act or FISMA. Two months ago, in August, 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 followed 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 federal networks against increasingly sophisticated attackers is not a trivial task. Yet, in the nearly seven years since FISMA was last updated in 2014, federal agencies still have the same vulnerabilities year after year – putting America's data at risk.

Today, we plan to take steps to remedy these systemic problems. The *Federal Information Security Modernization Act of 2021* incorporates recommendations from my bipartisan reports with Sens. Carper in 2019 and more recently, with Sen. Peters. This bill makes clear that:

- CISA will play a leading role in helping to secure federal networks, by ensuring that federal agencies and federal contractors provide notice to CISA when they suffer a cyber-attack.
- Agencies will provide notification to victims whose personal identifying information was compromised within 45 days.
- And updates the required notifications to Congress, in particular this Committee, when an agency suffers a major cyber incident.

And finally, while we planned to consider a bill regarding Inspector Generals, I appreciate Sen. Peters agreeing to hold that bill over to the next business meeting. We want that bill to be strongly supported by as many members of this Committee as possible. That

way, we send a strong bipartisan message of support to the IG community.

We're also considering three nominees for the DC Superior Court and one for the DC Court of Appeals, as well as three nominees for the Merit Systems Protection Board.

I want to speak briefly about the Merit Systems Protection Board, or MSPB. As many of us on this Committee know, the MSPB has been without a quorum since January 2017. The current backlog of cases is over 3,400; addressing this backlog will be no easy task.

While we are voting on three nominees to the MSPB today, I have strong concerns about Ms. Harris, who is nominated to be the Chair of the Board. Members of the MSPB must be steadfast in their impartiality. They must treat each federal employee that comes before them the same. Through her partisan statements, Ms. Harris has generated doubt as to whether she can meet this standard. So, I will not be supporting her nomination today. I do look forward to supporting both Raymond Limon and Tristan Leavitt who have both demonstrated a strong commitment to protect the Federal merit systems.

We also have four judicial nominations today. I plan to support the nominations of Ms. Puttagunta, Ms. Lopez, and Mr. Staples to be Associate Judges for the Superior Court of the District of Columbia. I will not, however, support Ms. Calderon's nomination to the DC Court of Appeals. I have concerns about her judicial philosophy. The DC court system has an important role to play in addressing the District's most pressing issues, including the recent increase in violent crime, and I hope that each of our Superior Court nominees are prepared to take on this role.

Thank you, Sen. Peters. I look forward to a robust discussion today.