COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

Hearing Statement of Chairman Bennie G. Thompson (D-MS)

Defending Against Future Cyberattacks: Evaluating the Cyberspace Solarium Commission Recommendations

July 17, 2020

At the outset, I want to acknowledge how fortunate we are, as Members of Congress, to have before us a whole-of-government, public-private sector blueprint for defending the nation against future cyber-attacks. Too often, thoughtful documents like this are the product of Monday morning quarterbacking that takes place after a catastrophic event has occurred.

After the September 11th attacks, the 9/11 Commission studied how the organization and policies of the Federal government led to its failure to predict, prevent, and prepare for the attacks, and made a series of recommendations to reorganize the government and build lacking capabilities.

After Hurricane Katrina, Congress identified critical deficiencies in Federal emergency management policy and overhauled it in the Post-Katrina Emergency Management Reform Act. After the Russian government attempted to meddle in our elections in 2016, I co-led a Task Force on Election Security to understand vulnerabilities in our election infrastructure, and we issued a report and recommendations to address them. Soon, I expect we will establish a Commission to study the failures of the Federal government that have led to its inept response to the COVID-19 pandemic.

We are lucky we are here today not to discuss a tragedy, but rather, how to organize the Federal government to effectively avoid one. At this time, the responsibility for leadership on Federal cybersecurity policy rests with Congress.

Although there are many well-intentioned, capable people working hard to advance sound cybersecurity policy throughout the executive branch, the lack of consistent leadership from the White House has stunted progress. Over two years ago, for example, the White House green-lighted the elimination of its Cyber Security Coordinator. The result is a lack of effective coordination among Federal agencies who compete for cybersecurity authorities, responsibilities, and associated budgets – and Federal agencies approaching Congress with conflicting priorities. The time has come for that to stop.

Toward that end, I appreciate and support the Commission's recommendation that Congress establish a National Cyber Director. I understand Congressman Langevin has authored legislation to implement that recommendation and has also submitted it as an amendment to the NDAA. I fully support both efforts.

I similarly appreciate the Commission's recommendations regarding strengthening the Cybersecurity and Infrastructure Security Agency and more clearly defining the roles and responsibilities of CISA and sector risk management agencies. Right-sizing CISA's budget and equipping it with the authorities necessary to carry out its mission to secure Federal networks, while also supporting critical infrastructure, has been a bipartisan priority of Committee Members.

I am particularly interested in hearing Ms. Spaulding's thoughts on these recommendations given her perspective as the former Under Secretary of the National Protection and Programs Directorate.

Additionally, I am interested in discussing Commission recommendations related to implementing a "carrot and stick" approach to encourage private sector collaboration with the Federal government's cybersecurity and defense efforts, particularly the proposed codification of "systemically important critical infrastructure."

Finally, I would be remiss if I did not address the Commission's observation that Congress' fractured jurisdiction over cybersecurity frustrates efforts to achieve a comprehensive, cohesive approach to cybersecurity. I agree. And while I disagree with the Commission's recommendation on that point, rest assured that I am working to address the underlying problem.

# # #

Media contact: Adam Comis at (202) 225-9978