COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Securing the DotGov: Examining Efforts to Strengthen Federal Network Cybersecurity

May 17, 2022

I would like to echo the comments my colleagues have made about the tragic mass shooting that occurred in Buffalo over the weekend. My thoughts are with the families of the victims. What happened was a flagrant act of terrorism, and this Committee will continue to do everything it is power to prevent future acts of such hateful violence.

Turning to the topic of today's hearing - We know that access to Federal agency networks is a top priority for our adversaries as they seek to gain information on government actions, and potentially, in some cases, develop capabilities for destructive attacks. Therefore, we must improve our ability to prevent such intrusions and to discover and mitigate them promptly when any intrusion does occur.

This requires a whole-of-government effort that brings together agencies across the Federal government to support the shared mission of defending our networks. I am glad that Chairwoman Clarke and Ranking Member Garbarino have gathered some of the key players here today to update the subcommittee on how much progress they have made in enhancing Federal cybersecurity and to help us understand what additional authorities and resources they may need to fulfill their mission.

President Biden's Executive Order 14028, signed just over a year ago, is an extremely ambitious effort, and I have been impressed with the speed at which agencies have worked to meet its tight deadlines. This type of urgency is exactly what we need to address a national security problem that has not previously been adequately addressed. But, as we exit the initial phase of implementation, we must make sure we sustain the effort going forward. For example, as the SolarWinds intrusion demonstrated, our Federal networks are only as secure as our most vulnerable software supplier.

Under the E.O., NIST has undertaken important work to update guidance on supply chain security standards, but we still need that work reflected in updated language for Federal contracts. And Federal agencies will need to partner with the private sector to ensure these heightened standards are implemented and enforced.

Additionally, we have seen that Federal agencies have been slow to adopt basic cyber hygiene practices like multi-factor authentication, so we must expedite efforts to provide them the resources and support needed to match the same standards we are urging for our constituents. Ultimately, a challenge with any security problem is that you can rarely eliminate the threat, and this is particularly true in the cyber realm where the threat is always evolving.

But, our goal must be for us to not need another historic executive order on this topic in the future, but instead develop the structures and policies that will enable the Federal government to continually improve its security to stay ahead of our adversaries.

I believe that the expanded authorities we have provided for CISA, the creation of the Office of the National Cyber Director, and this executive order all bring us closer to that point, and this hearing should help enable the subcommittee to better understand how we can partner with the Administration to continue the tremendous progress we have made so far.

# # #

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