COMMITTEE ON HOMELAND SECURITY

FOR IMMEDIATE RELEASE

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

Evolving the U.S. Approach to Cybersecurity: Raising the Bar Today to Meet the Threats of Tomorrow

November 3, 2021

I would like to thank National Cyber Director Inglis and CISA Director Easterly for participating in today's hearing on how the Federal government is maturing its approach to securing Federal networks and critical infrastructure. At the outset, I would like to commend the Administration for its steadfast commitment to confronting the cybersecurity challenges facing the nation, and I would like to thank both of you for the important role you play.

This Committee has a long history of bipartisan collaboration in support of advancing strong, sound cybersecurity policy, and we look forward to working with both of you in your respective roles. Last Congress, Members of the Committee worked together to raise CISA's funding, expand CISA's authorities, and authorize the National Cyber Director.

With the support of this Committee, CISA worked tirelessly with State and local election officials to ensure the most secure election in history – during a global pandemic no less. But late last year, we learned that the Russian government conducted a sophisticated supply chain attack and gained access to our government and private sector networks. Only months later, Microsoft disclosed that Chinese hackers exploited multiple zero-day vulnerabilities in Microsoft Exchange Servers to gain access to emails and maintain persistent access to the networks.

A series of high-profile ransomware attacks threatening the fuel and food supply followed. And just yesterday, voters went to the polls to cast their ballots even as efforts to push the Big Lie and erode public confidence in democratic institutions persist.

These events forced three important conversations:

- How do we activate resources and authorities quickly to modernize Federal network security programs?
- Does the Federal approach to securing critical infrastructure – which relies heavily on voluntary frameworks – serve the national security interested of the American people?
- How do we protect public confidence in our democratic institutions, particularly our elections?

To its credit, the Administration has confronted these challenges head on, laid out a bold agenda, and put its money where its mouth is.

From the ambitious Executive Order on Improving the Nation's Cybersecurity, to the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, to the pipeline security directives, the Administration is aggressively leveraging existing authorities to raise the nation's cybersecurity posture. Last week, the White House asked Congress to expand the Environmental Protection Agency's ability to regulate cybersecurity for the water sector.

Moving forward, I will be interested to know whether you expect the Administration to leverage or seek similar authorities to impose mandatory cyber standards on other sectors, and if so, what you expect the role of your organizations to be in that process. Given my role on both this Committee and the January 6th Select Committee, I am disturbed by how disinformation fosters conspiracy theories, divides us, and makes us doubt our democratic institutions. I will be interested to understand how CISA's maturing its election security activities, related to both the security of election infrastructure and its rumor control efforts.

While I appreciate the Administration doing what it can by leveraging the authorities it has, this Committee is working hard to provide many of the additional authorities necessary for CISA to take on the challenges ahead. For example, bipartisan Members of the Committee offered amendments to the NDAA that would establish a mandatory cyber incident reporting framework, authorize the CyberSentry program, and establish the Joint Collaboration Environment. I'm hopeful that today we can discuss how you will implement those measures when they are enacted into law, as I expect them to be.

# # #

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