COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

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

Evaluating Federal Cybersecurity Governance

October 25, 2023

At the start of last Congress, the SolarWinds Supply Chain compromise laid bare unacceptable gaps in our approach to securing Federal networks.

The capabilities of our adversaries and the technology we relied on had evolved, but our approach to security had not. We failed to appreciate the challenges associated with securing - and maintaining visibility - in cloud environments; we did not have policies in place to ensure the security of software that underpins our information systems; and we tolerated a sluggish rate of maturation for our Federal network security programs. The SolarWinds compromise jolted Congress and our partners in the Administration into action, and as a result we have made historic progress modernizing the Federal government's approach to cybersecurity.

The ambitious goals President Biden set out in Executive Order 14028, *Improving the Nation's Cybersecurity*, and the National Cybersecurity Strategy, coupled with a long overdue injection of resources and authorities from Congress, have put the Federal government's networks on a more secure path. But I am concerned that the politicization of the Cybersecurity and Infrastructure Security Agency (CISA) by some of my colleagues could jeopardize the progress we have made over the past three and half years.

Last month, a concerning number of Republicans, including some on this panel and the new Speaker, voted to cut CISA's funding by 25 percent. To further complicate matters, the Continuing Resolution - which is sustaining existing Federal cybersecurity efforts - will expire in less than 25 days. Right now, there is no clear path for providing full-year funding. We already know that the world's most sophisticated hackers are interested in and capable of compromising Federal networks, and they won't take a break just because Republicans can't figure out how to fund the government.

Particularly in light of escalating global conflicts, we must remain vigilant in our commitment to providing the funding necessary to fully implement President Biden's Federal network security goals. Beyond the issue of resources, I want to emphasize the importance of clear, transparent, and deliberate communication with the private sector as the Administration executes the directives under the Executive Order and the National Cyber Strategy.

By demanding better security practices from those who sell information technology to the government, the Administration can drive critical changes in the market that will benefit everyone – but only if its private sector partners understand and are prepared to meet these new requirements.

This Administration is advancing cyber policy at unprecedented speed – and I support these efforts. But we must be careful not to sacrifice sound policy for speed. Toward that end, I will be interested in understanding how the Administration has gathered feedback from its private sector partners to refine and adjust new security policies.

Finally, I look forward to learning how recent investments modernizing Federal network security programs and expanding endpoint detection tools are driving down risk and improving our ability to rapidly detect malicious activity on Federal networks.

# # #

Media contact: Adam Comis at 202-225-9978