COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Cybersecurity & Infrustructure Protection Subcommittee

Rep. Robert Menendez Opening Statement

Evaluating CISA's Federal Civilian Executive Branch Cybersecurity Program

September 19, 2023

Two and a half years ago, the SolarWinds supply chain attack forced the Federal government to overhaul its approach to securing its networks and supply chains.The Biden-Harris Administration made revamping Federal network security a top priority, issuing an ambitious Executive Order that brought to bear the full resources of every Federal agency with a cybersecurity mission. Together with Congress, the Administration made historic investments in improving Federal network security.

Not since the 2015 Office of Personnel Management breach had there been as much momentum for change in how we secure Federal networks. While President Biden and Congress certainly deserve credit for giving needed attention to Federal network security, it is critical that we continue our work to modernize federal network security to avoid crisis-driven policymaking.

We must ensure that the programs we rely on to secure our networks can adapt to and integrate with new technologies and modern network architectures.

And we must endeavor to stay a step ahead of our adversaries, building upon our recent momentum to better detect malicious activity quickly and mitigate the risks posed by cyber intrusions.

CISA plays a central role in securing our Federal networks as the administrator of the National Cybersecurity Protection System, commonly referred to as NCPS, and the Continuous Diagnostics and Mitigation program, commonly referred to as CDM. These programs complement CISA's other important powers, including the authority to issue security guidance and best practices, Binding Operational Directives, and Emergency Directives, which require agencies to take expedited action to secure their networks against a pressing threat or vulnerability. Over the past two and a half years, CISA has laid out its plans to modernize both NCPS and CDM programs.

Earlier this year, CISA announced plans to sunset and replace its EINSTEIN intrusion detection system - which has limited effectiveness against novel threats and newer network architectures – and shift remaining NCPS capabilities to a new program called the Cyber Analytics and Data System (CADS). Together, the legacy EINSTEIN capabilities and CADS will become the Joint Collaboration Environment, commonly referred to as JCE, which CISA predicts will be a "best-in-class analytic environment" that utilizes increased automation to more efficiently analyze classified and unclassified data. JCE holds tremendous promise, but successful implementation requires a clear vision and buy-in from both Federal and private sector partners.

CISA has also worked to rapidly mature its CDM program to ensure that its Federal customers can tailor it to accommodate their unique security requirements. CDM is limited, however, in that it is deployed on IT technologies, not operational technology or Internet of Things devices. Moreover, the Government

Accountability Office recently found that CISA lacks the authority to test CDM tools on agency networks, which undermines its ability to ensure those tools are working as anticipated. I am interested in learning from witnesses today how we can improve the security value of both programs.

Before I close, I want to remind my colleagues that government shutdowns are bad for Federal network security. We are nevertheless two weeks away from government funding running out. During the last shutdown – which lasted 35 days – CISA issued its first Emergency Directive to Federal agencies ever. Having employees and IT contractors across the government – and at CISA – furloughed at the time was not helpful. A continuing resolution would also impair CISA's critical work, as it would restrict CISA's ability to start new programs that match the current threat environment.

It is detrimental to our national security to slow investments in our Federal network security programs at such a critical moment in their maturation. Moving forward, the House and Senate need to pass a Homeland Security appropriations bill that provides needed funding to CISA to carry out its vital missions. Now is not the time to take our foot off the gas.

# # #

Media contact: Adam Comis at 202-225-9978