



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson***DHS' Efforts to Secure .Gov***

June 24, 2015 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Cybersecurity, Infrastructure Protection, and Security Technologies subcommittee hearing entitled “DHS’ Efforts to Secure .Gov”:

“I thank the leadership of this Subcommittee for continuing to focus on our nation’s most pressing cyber vulnerabilities - protecting our nation’s critical infrastructure systems, and protecting citizens and federal workers and their personal information. Over the past few months, the Committee has found the repeated news that some of our most valuable government agencies have been infiltrated, and government employees’ detailed personal information have been exposed quite appalling.

We have seen the Internal Revenue Service breached. At the Defense Department, Secretary Carter has told us about the Russian’s hacking from earlier this year, and now, we have a multi-layered exposure of federal workers exposed in an Office of Personnel Management incident. Our networks and databases cannot be protected by one protocol, one sophisticated procedure, or one magic arrow. We have cybersecurity programs in place, but for them to take hold, either in the private sector or across government agencies, it will require leadership, cooperation, and accountability. For example, The President’s cybersecurity Executive Order 13636 has charged the Department of Homeland Security to be the motivator, teacher, and implementer of the art and science of network and database security, across the federal government.

However, for DHS to fulfill this mission, it has to engage with both the public and private sectors. I want to hear more from Dr. Ozment on how DHS is fulfilling this mission, and how it has responded to previous intrusions. It is important for all of us to remember that cybersecurity is a shared responsibility, and that no single approach can protect us completely. Cyber threat protection is a complex and incomplete process and it crosses several important intersections, especially regarding privacy and civil liberties.

As people and government become more dependent on technology, technology-based opportunities for crime, espionage, and physical disruption will most certainly increase. Today, some contend that greater security means ceding some degree of personal privacy, or vice versa. But in my book, cybersecurity enables privacy—because it protects individuals, companies, and governments from malicious intrusions. Privacy and security are not competing interests; we can and must do both. The United States can set a positive example regarding the role that cybersecurity standards play globally, for both industry and government. If we can develop effective, secure protocols and standards that are easily implemented, it will represent an important opportunity for U.S. products around the globe.

Finally, I would be remiss if I did not mention the cost of these programs discussed today. All of this cybersecurity effort does not come cheap. While the majority has seen fit to increase cybersecurity funding by large amounts in some cases, House and Senate Republicans have started to show how they plan to budget at discretionary levels for other programs.

Compared to the President’s Budget, their budget will force cuts in areas critical to the economy, as well as in national security priorities. Homeland security, peacekeeping efforts, defense and foreign assistance will be impacted. These funding levels are the result of Congressional Republicans’ decision to lock in the funding cuts imposed by sequestration. As we all know, sequestration was never intended to take effect: rather, it was supposed to threaten such drastic cuts to both defense and non-defense funding that policymakers would be motivated to come to the table and reduce the deficit through smart, balanced reforms. Unfortunately, the bills and appropriations targets released to date double-down on a very different approach.”

#

FOR MORE INFORMATION: Please contact Adam Comis at (202) 225-9978

H2-117, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
<http://chsdemocrats.house.gov>