FOR IMMEDIATE RELEASE

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

Assessing the State of Federal Cybersecurity Risk Determination

Subcommittee on Cybersecurity & Infrastructure Protection

July 25, 2018

At the outset, I would like to echo Ranking Member Richmond's disappointment that we are heading into August recess without making any meaningful progress on reauthorizing the Chemical Facility Anti-Terrorism Standards Program (CFATS), which expires in less than 6 months. As far as I know, the CFATS program has bipartisan support on this Committee. It is also popular with the regulated community, and, most importantly, makes our communities safer. Given the limited number of legislative days left, I hope this Committee acts quickly when we return in September to fulfill our obligations as authorizers and put CFATS on the track to reauthorization.

Turning to the subject of today's hearing – although I am pleased that OMB and DHS have undertaken a review of the risk determination and acceptance choices across the Federal government, I am troubled that many of our cybersecurity capabilities are not as mature as they ought to be.

When I joined the Select Committee on Homeland Security in 2003, every expert I heard from told me that the Federal government was ten years behind where it should in with respect to cybersecurity. Despite the investments we have made since then, it seems we are in the same boat – 10 years behind where we need to be.

Federal agencies still struggle to access timely, actionable threat information and share it enterprise-wide. Agencies still do not have full visibility of what is happening on their networks or who has access to different pieces of information. And we still have not figured out how to strategically allocate funding to address risk.

Despite the devastating data breaches like the 2015 Office of Personnel Management heist of the personal information of 22.1 million people, non-defense agencies spent less than $51 million encrypting data rest in FY 2017.

Meanwhile, of the $80 billion we spend annually on IT systems across the Federal government, 80 percent is spent maintaining legacy systems that are more vulnerable and less secure. We need to start putting our money where the risk is. This is not the first time we have heard these recommendations.

So, there is one thing I would like to know from our witnesses today: how can the Federal government finally jump the ten-year gap between where we are and where we should be?

I know it will take technology. I know it will take money. And, importantly, I know it will

take leadership.

I am concerned that the White House has limited its ability to lead as effectively as it could in this space by eliminating the Cybersecurity Coordinator position and dragging out the appointment of the Federal CIO and CIOs and large agencies.

Nevertheless, as Members of Congress, we will continue our rigorous oversight to hold the Administration accountable for the action items outlined in the Federal Cybersecurity Risk Determination Report and Action Plan.

# # #

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