FOR IMMEDIATE RELEASE

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

The Current State of DHS' Efforts to Secure Federal Networks

Subcommittee on Cybersecurity & Infrastructure Protection

March 28, 2017

Cyberattacks against Federal networks and the nation have been increasing in frequency in recent years, with high profile breaches of federal systems at the White House, State Department, Veterans Affairs, and the Office of Personnel Management (OPM).

These breaches, many of which are believed to be carried out at the direction of state actors, have called into question the ability of the Federal government to adequately secure its data and networks.

For instance, there was the massive OPM breach that occurred two years ago. In that attack, the personnel records of at least 22 million people were stolen. These records included very sensitive and personal information about not just Federal employees and contractors but also about their families and friends. Hackers believed to be working for the Chinese government carried out this malicious attack.

Last week, the Committee heard from national security experts about the growing and gathering threat posed by state actors—most notably China, Iran, North Korea, and Russia. I was struck by the testimony of Dr. Frank Cilluffo from the George Washington University who characterized the threats posed by these countries in the following way-- "Russia is the most capable, China is very active in computer network exploit or espionage activity," and North Korea and Iran are the most likely "to turn to computer network attacks" to damage our systems.

With respect to Russia, the threat posed by Vladmir Putin has become a "kitchen-table" topic. Americans want to know more about the cyber hacking and influence operation that Putin directed against our democracy in the lead up to the 2016 election.

They also want to know if there was any collusion between U.S. persons and Russian operatives to carry out what FBI Director James Comey has called a "successful" operation. These are not minor or trivial concerns. The Russians, as Director Comey has determined, are proud to have "sewed doubt about the nature of our democratic process" and because they were successful, he warned that "they'll be back."

Mr. Chairman, I was pleased to hear you acknowledge at last week's hearing that these actions by Russia were an invasion of the privacy of citizens and that they undermined our democratic institutions and elections.

Given that the House Intelligence Committee's bipartisan inquiry seems to be unraveling at the hands of its chairman, now is the time for Members of Congress—regardless of party—to stand together in support of a non-partisan commission, one akin to the 9/11 commission.

Turning back to the witnesses before us today, I look forward to hearing from the panel on how DHS is progressing in its Federal cybersecurity role and what more can be done within DHS and across the Federal government to better mitigate, respond to, and recover from attacks on federal information systems.

# # #

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