NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member

FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Cloud Computing: What are the Security Implications?

October 6, 2011 (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 “Cloud Computing: What are the Security Implications?”:

“Before I begin my statement for today, I’d just like to say a word on the release of your Caucus’ Cyber Task Force recommendations yesterday. As we all know, Cyber is an emerging homeland security threat that warrants timely bipartisan action from Congress. The stakes are high, as federal networks alone have seen a 650-fold increase in cyber attacks over the past 5 years. The President has submitted to Congress a comprehensive plan, including a legislative proposal. I’m not sure that this partisan product adds much to the discussion, especially in the absence of a legislative proposal.

Mr. Chairman, thank you for holding today’s hearing to examine the security implications of cloud computing. Cloud computing can and does mean different things to different people. The National Institute of Standards and Technology (NIST) has published a definition that provides a starting place for discussing and defining security needs.

But not everyone agrees with or conforms to the NIST definition. So as of today, the Federal government and industry have not reached agreement about uniform rules and standards that should be adopted to secure the information in the cloud. This is not something that can be left up in the air.

While I embrace technological progress, I also know that every new technology presents great possibilities as well as great challenges. In our eagerness to jump on the bandwagon, we often forget to ask about the destination of the wagon, the cost of the journey and the roads we will take along the way.

As we embark on this new journey of migrating information to the cloud, we must not repeat mistakes of the past. We must know more about some of the claims that are made. For instance, I am told that the cloud will produce cost-savings and create efficiencies.

I am told that these benefits will be achieved by eliminating the need for data centers, computer hardware and other public and private sector operations that employ thousands of people. I have to ask about these displaced people. And while every new technology creates displacement, it also provides opportunities. So we must ask what new opportunities will be provided and who will benefit?

Finally, as cloud computing increases the Federal government’s ability to communicate effectively; we must ask how this increased ability to communicate will affect the security of governmental operations. Mr. Chairman, without clear standards and uniform rules we cannot begin evaluate how the security of government data will be affected by cloud computing.

Additionally, we must remember that cloud computing must be aligned with the Federal Information Security Management Act (FISMA). Given that the Federal government currently uses the services of external vendors to manage its cloud operations, we must ask how these businesses will comply with FISMA regulations governing auditing and security requirements. Industry cannot effectively compete without understanding the potential regulatory environment that will be caused by widespread use of cloud computing in the Federal government.

Mr. Chairman, there are many questions that must be resolved. However, I am certain that our witnesses today will be able to shine some light into the cloud."

# # #

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

United States House of Representatives
Committee on Homeland Security
H2-117, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
http://chsdemocrats.house.gov