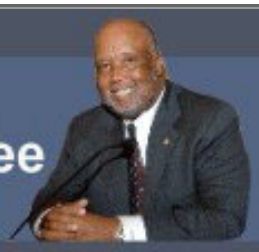
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?

November 13, 2013 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee hearing entitled "Cyber Side-Effects: How Secure is the Personal Information Entered into the Flawed Healthcare.gov?":

"I understand that this hearing will discuss the Department of Homeland Security's role in the Affordable Care Act. The role played by DHS is two-fold. First, the Department is responsible for verifying that anyone who applies for benefits under the ACA is a citizen or legal resident. This function, required by the ACA, is very similar to the information required under E-Verify. The department performs this function thousands of times each day and transmits the information to any government agency or employer that needs it.

I am sure we all remember the beginning of the E-Verify program. Just a few years ago, my friends on the other side of the aisle sought to expand E-Verify. At that time, many critics believed E-Verify was a deeply-flawed program that relied on inaccurate government databases and added unnecessary costs to businesses. We called attention to flaws in the computer systems and databases that E-Verify relied upon. The deficiencies in those systems were fixed.

Today, E-Verify has become an ordinary part of the verification process used by businesses and governments to assure that people are eligible to work in the United States. I do not recall efforts to repeal E-Verify because of its faults.

The SAVE system, used in the ACA, functions in much the same way as E-Verify. It seems that my colleagues have expressed concerns about the other role DHS plays in the implementation of the ACA. Those concerns have been examined at two subcommittee hearings in this Committee. Based on those hearings, we know that DHS did not have any role in the planning or implementing the Healthcare.gov website.

Some of my colleagues have indicated that DHS should assure the safety and security of the personal information placed on Healthcare.gov. While this is an interesting proposition, there is no law requiring that DHS play such a role. DHS has a few responsibilities in the cyber area. First, DHS is responsible for observing, reporting and acting upon threats to the federal computer network system.

Second, DHS is responsible for assuring that all Federal agencies are in compliance with FISMA—the federal law that establishes benchmarks and standards for computer system security within the Federal government. In sum, DHS is responsible for assuring that HHS followed the correct protocols in establishing the system and DHS would be ready to respond if the system were hacked.

But DHS does not have an ongoing role with the security of the Healthcare.gov system.

If my colleagues believe DHS oversight would be beneficial in assuring the privacy and security of the information contained in the Healthcare.gov system, I would suggest that we explore that option.

But I am not aware of any law that suggests that role for DHS, and I do not believe the consideration of such a role is the purpose of today's hearing. It seems that the purpose of today's hearing is to raise concerns about the protection of the privacy and security of personal information. Several committees in the House of Representatives have had hearings on this same topic.

Although it is my understanding that DHS has a very small role in assuring the privacy and security of a website established by another agency, I look forward to hearing from the witnesses called here today.

Finally, Mr. Chairman, I do not think that the discussion today can ignore the fact that this website was put together using over 50 contractors. s we know from this committee's recent mark-up of a bill on the cyber security workforce, the federal government is woefully deficient in hiring and retaining cyber professionals. The oversight conducted by this committee over several years has found one IT system after another that has failed to perform or failed to be completed after millions of dollars have been spent.

The list of computer failures is long and stretches through a few administrations. The list includes—SBI, Emerge, RAMP—and several other IT solutions that did not have names, did not work, but did cost a great deal of money. I am not here to point a finger at DHS. I am certain that DHS is not the only federal entity that has been plagued by the failure of computer contracts to deliver what was promised.

So Mr. Chairman, while I look forward to the discussion today, I hope that at some point we can light a candle instead of continuing to curse the darkness. Those of us in Congress need to come to grips with the notion that computers are not going away and we must take proactive steps to assure that some office or agency is the repository of cyber expertise and knowledge.

That agency must be able to advise other agencies on everything from drafting a solicitation for a computer system to oversight of the installation of the system. It must be the federal IT help desk and information library.

We need to think about a new approach that will save money and work for the American people. Or we can keep doing what we have been doing—spending money, making mistakes, wondering what went wrong and trying to figure out who to blame. Mr. Chairman, the people deserve a government stays open, works together, solves problems and spends money wisely. I think this is the perfect time to show that we are that government."

# # #

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