ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051

http://oversight.house.gov

Opening Statement
Rep. Elijah E. Cummings, Ranking Member

Hearing on "Examining ObamaCare's Failures in Security, Accountability and Transparency"

September 18, 2014

One of our most important jobs in Congress is to help protect the interests of the American people. They demand that the government and private companies safeguard their personal information—their social security numbers, their credit cards, and their health information.

Nobody wants to get a call from a credit card company saying, "your personal information has been compromised." It can upend your entire life, and it can cause serious financial problems for years.

I believe our Committee has the potential to perform a valuable function in this area. With our extremely broad jurisdiction over multiple federal agencies and corporate entities, we can help promote robust security standards across the entire government and private sector. To date, however, we have not fulfilled this potential.

Today's hearing is our 29th on the Affordable Care Act (ACA) and our sixth on HealthCare.gov. I completely agree that the ACA website must be secure. That is why I am so heartened that, despite all of the challenges with the rollout last year, nobody's personal information has been compromised to date as a result of a malicious attack. Now, that could change, so we have to remain vigilant, but so far no attacks have been successful in that regard.

There certainly have been attempts. Last week, the Centers for Medicare and Medicaid Services reported that hackers uploaded malware onto a server. But there are several key facts to know about that attack.

First, it was not directed at HealthCare.gov alone, but at a much wider universe of targets. Second, the server that was attacked was a "test" server that had no personal information on it. Third, and most important, nobody's personal information was compromised as a result.

That incident was investigated by the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security. The Director of that team, in her written testimony for today, reports that "there is no indication that any data was compromised as a result of this intrusion."

Although our Committee has spent a tremendous amount of time focusing on the Affordable Care Act and its website—where no cyber attacks have compromised anyone's personal information to date—we have been disregarding much more serious attacks that have actually compromised a massive amount of personal information. We are talking about hundreds of millions of people.

For example, on January 14, more than eight months ago, I sent a letter requesting a bipartisan hearing with senior officials from Target. As I wrote:

> [U]p to 110 million Americans were subjected to one of the most massive information technology breaches in history when their credit, debit, and other personal information reportedly was compromised.

On September 9, I sent a letter requesting a bipartisan hearing on a major data security breach at Community Health Systems, the nation's largest for-profit hospital chain. I explained that "hackers broke into its computers and stole data on 4.5 million patients." As I noted, this was "the largest hacking-related health information breach ever reported."

On September 11, I sent a letter requesting a bipartisan hearing to examine the recent security breach at Home Depot. I explained that Home Depot "has more stores in the United States and a higher total annual sales volume than Target," and it "appears to have experienced a data security breach for a longer period of time than the data security breach that occurred at Target."

And just this Monday, I sent a letter requesting a deposition with the CEO of USIS, the company that conducts more background checks for the government than any other contractor, and which had its own breach this summer. As I wrote:

> [A]lthough press accounts have reported that the attack may have compromised the personal information of up to 27,000 federal employees, government cyber security experts now believe this number is a floor—not a ceiling.

In response, I received a letter back from the Chairman yesterday thanking me for my requests over the past year and acknowledging that "these serious incidents merit further review." Mr. Chairman, I thank you for that, and I hope we can start on this right away.

Let me close by highlighting that this is much broader than HealthCare.gov. GAO, which is also represented here today, warns that the number of cyber attacks is increasing against targets across the federal government, and obviously the same is true of the private sector.

So oversight is certainly called for, and I hope our Committee seizes the opportunity and rises to the challenge. Thank you.

Contact: Jennifer Hoffman, Communications Director, (202) 226-5181.