JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

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
MINORITY (202) 225–5051

http://oversight.house.gov

Opening Statement
Ranking Member Elijah E. Cummings

Hearing on "OPM: Data Breach"
June 16, 2015

The recent cyber attack against the Office of Personnel Management (OPM) is the latest in a series of aggressive attacks against our nation in both the public and private sectors. I would like to put up a slide that lists some of the most significant data breaches over the past few years.

Anthem—80 million people. JPMorgan—76 million. Target—70 million. OPM—at least 4 million so far. Then there was the Postal Service, Sony Pictures, and USIS. And this is not a comprehensive list by any means.

Ladies and gentlemen, when you see this list, the picture is clear: the United States is under attack. Sophisticated cyber spies—many from foreign countries—are targeting the sensitive personal information of millions of Americans. They are attacking our government, our economy, our financial sector, our healthcare system, and virtually every aspect of our lives.

For more than two years, I have been pressing for our Committee to investigate these cyber attacks. So I thank the Chairman for holding today's hearing, and I hope we will hold similar hearings on many of these other attacks as well.

With respect to the attack against OPM, my primary concern is who was targeted—government workers—and what foreign governments could do with this information. I have several questions for OPM. How many federal employees were affected? What kind of information was compromised? And what steps are being taken to help these employees now?

I also want to know how these attackers got inside OPM's networks. Last year, cyber attackers penetrated the networks of USIS and KeyPoint, two contractors that performed background checks for security clearances on behalf of OPM.

One of the most critical questions we have today is this—did these cyber attackers gain access to OPM's data systems using information they stole from USIS or KeyPoint last year? Did they get the keys to OPM's networks from one of its contractors?

Mr. Chairman, I asked you to invite both KeyPoint and USIS representatives here to testify today. You agreed to invite USIS, but last night they refused, just as they have refused repeated requests for information over the past year. They did not offer someone else they thought was more appropriate.

I do not say this lightly, Mr. Chairman, but I believe USIS and its parent company may now be obstructing this Committee's work. We have suggested previously that the Committee hold a transcribed interview and, given the history of non-compliance at USIS, I believe this may be one of the only ways to obtain the information we are seeking.

Mr. Chairman, over the last two years, I have also been pressing to investigate ways to better protect personal information that belongs to the American people—their financial records, medical records, credit card information, Social Security Numbers, and a host of other information they want to keep secure.

I sought advice from some of the nation's top information security experts in private business and government. These experts warn that we cannot rely primarily on keeping the attackers out. We need to operate with the assumption that the attackers are already inside.

Last week, one of the world's foremost cyber security firms—Kaspersky Labs—was penetrated in a cyber attack. And according to FireEye, one of the companies my staff spoke with, the average amount of time a hacker remains undetected is more than 200 days.

Obviously, we need strong firewalls and other defenses to keep attackers out, but experts recommend much more aggressive measures to wall-off—or segregate—data systems to minimize the impact of inevitable data breaches in the future. Practices like data masking, redaction, and encryption must become the norm, rather than the exception.

Finally, we need to remember who the bad guys are here. They are not U.S. companies or federal workers who are trying to keep our information safe. The bad guys are the foreign nations and other entities behind these devastating attacks. According to law enforcement officials, North Korea, China, Russia, and Iran are among the most advanced persistent threats to this nation's cyber security.

So, as we move forward today, I want to caution everyone that as much as we want to learn about this attack, we have to do so in a responsible way. A lot of the information about the attack is classified, and the last thing we want to do is give our enemies information or compromise active law enforcement investigations. We are having a classified briefing for Members at 1 p.m. today, so I encourage everyone to attend that.

Mr. Chairman, thank you for the bipartisan approach you have taken on this issue, and I hope we can continue to investigate these other breaches to identify common threats against our country and the best ways to counter them. We need to work together on this.

Contact: Aryele Bradford, Deputy Communications Director, (202) 226-5181.