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: Part II"
June 24, 2015

We are here today because foreign cyber spies are targeting millions of our federal workers. They are hacking into our data systems to get information about these employees—private information about them, their family, their friends, and their acquaintances. And they may try to use that information in their espionage efforts against U.S. personnel and technologies.

Mr. Chairman, I want to start by thanking you. Last week, we held a hearing on the cyber attacks against OPM, and this week we have an opportunity to hear from OPM's two contractors that also suffered major data breaches—USIS and KeyPoint. Some people in your shoes might have merely criticized the agency without looking at the whole picture, but you agreed to my requests to bring in the contractors, and you deserve credit for that.

On Monday night, I received a letter from USIS representatives finally providing answers to questions I asked more than seven months ago. Their letter disclosed that the breach at USIS affected not only DHS employees, but our immigration agencies, our intelligence community, and even our police officers here on Capitol Hill. My immediate concern was for the employees at these agencies, and I hope they were all alerted promptly. But there is no doubt in my mind that USIS officials never would have provided that information unless they were called here to testify today. So thank you for that, Mr. Chairman.

I have some difficult questions for USIS today. I want to know why this company paid millions of dollars in bonuses to its top executives—after the Justice Department brought suit against the company for allegedly defrauding the American taxpayers of hundreds of millions of dollars. I want to know why USIS used these funds for bonuses instead of investing in adequate cyber security protections for the highly sensitive information our nation entrusted to it.

Mr. Gianetta, I want to know if you, as the Chief Information Officer at USIS, received one of those bonuses. I understand that you just returned home from Italy, so this is probably the last place you want to be. I also understand you are leaving the company in a matter of weeks. But I also want to know why USIS has refused for more than a year to provide answers to our questions about the Board of Directors of its parent company, Altegrity.

Mr. Hess, I also have difficult questions for KeyPoint. At last week's hearing, I said one of our most important questions is whether these cyber attackers were able to penetrate OPM's

networks using information they obtained from one of its contractors. As I asked last week, did they get the keys to OPM's networks from its contractor?

Yesterday, Director Archuleta answered that question. Appearing before the Senate Appropriations Committee, she testified that "the adversary leveraged a compromised KeyPoint user credential to gain access to OPM's network."

So the weak link in this case was KeyPoint. Mr. Hess, I want to know how this happened. Although I appreciate that OPM continues to have confidence in your company—unlike USIS—I also want to know why KeyPoint apparently did not have adequate logging capabilities to monitor the extent of data that was stolen. Why didn't you invest in these safeguards?

Mr. Chairman, to your credit, one of the first hearings you called after becoming Chairman was on the risks of third-party contractors to our nation's cyber security. At that hearing on April 20, multiple experts explained that federal agencies are only as strong as their weakest link. If contractors have inadequate safeguards, they place our government systems—and our workers—at risk.

I understand we have several individuals here sitting on the bench behind our panel of witnesses who may be called to answer questions if necessary, including Mr. Job, who is the CIO of KeyPoint, and Mr. Ozment from the Department of Homeland Security. Thank you, Mr. Chairman, for allowing them to be here.

As we move forward, it is critical that we work together. We need to share information, recognize when outdated legacy systems need to be updated, and acknowledge positive steps when they occur. Above all, we must recognize that our real enemies are outside these walls—they are the foreign nation states and other actors that are behind these devastating attacks.

Thank you, Mr. Chairman.

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