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 Robin Kelly

Hearing on "Federal Cybersecurity After the OPM Data Breach: Have Agencies Learned their Lesson?"
Subcommittee on Information Technology

November 16, 2016

Thank you Chairman Hurd, for holding this important hearing on the state of federal cybersecurity in the wake of the OPM data breach and I thank the witnesses for joining us today to testify.

Cybersecurity is a critical concern for both the public and private sectors, as the recent breaches affecting millions of people at the Office of Personnel Management (OPM) and Yahoo illustrate.

In our investigation of the OPM data breach, we discovered that a sophisticated, nation-state adversary targeted both OPM and private sector companies performing services for the government in order to steal sensitive information about federal employees. In fact, the OPM breach was achieved using credentials taken from one of OPM's contractors.

The Minority staff memorandum concluded that "federal cybersecurity is intertwined with government contractors, and that cyber requirements for government contractors are inadequate."

In the past two years, Congress passed, and President Obama signed into law, the Federal Information Security Modernization Act of 2014, known as FISMA and the Federal Cybersecurity Enhancement Act of 2015, known as the FCEA. These laws create stringent standards for agency information security programs and will implement innovative technologies such as the EINSTEIN federal detection and intrusion prevention system, as well as multi–factor authentication.

Congress has a responsibility to ensure that agencies are complying with these enacted pieces of legislation.

This past July, the Committee sent bipartisan letters to the 24 CFO Act agencies, requesting information on FISMA compliance and FCEA implementation progress.

We are here today to discuss agency compliance with FISMA and agency progress on the upcoming December 2016 deadline for FCEA implementation.

I understand that the Office of Management and Budget recently issued a report on FISMA required independent evaluations of agency information security systems for Fiscal Year 2015. This report shows a decline in agency FISMA scores over the past year for our three witness agencies here today. Each agency's independent evaluation of their information security programs highlights the strengths of their individual programs and areas that can use improvement.

One of the key aspects of FISMA is moving from a check–the–box mentality of cybersecurity to an approach of continuous monitoring and reporting. I would like to hear from our witnesses as to how Congress can help them achieve that goal.

I would like to hear if any challenges are being encountered in the implementation of FCEA-required programs and practices.

I want to again thank our witnesses for their testimony today. Effective federal cybersecurity is possible through cooperation between agencies and Congress.

I look forward to having a discussion on how we can better work together to develop policies that will secure not only agency systems, but private sector systems as well.

Thank you, Mr. Chairman. I've long said that the federal government needs to lead by example when it comes to improving our national cybersecurity. And I'm proud of the steps we've taken in this subcommittee towards this goal. But it's clear that we have much more work ahead. I look forward to continuing our work together next Congress.

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