

## OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)  
Committee on Science, Space & Technology

*Is the OPM Data Breach the Tip of the Iceberg?*  
Joint Subcommittee Hearing

July 8, 2015

Thank you Chairwoman Comstock and Chairman Loudermilk for holding this hearing on the recent OPM data breach.

Even though we will continue to learn more details about the breach, we already know that millions of Americans' personal information was compromised. This number includes current and retired federal employees as well as the family members, friends, and co-workers of federal employees.

There are valid concerns about hackers using this data for criminal purposes. Additionally, since security clearance background investigation information was compromised, there are also serious national security concerns.

It is frustrating to learn that OPM knew that they had serious information security systems problems long before this breach. Although addressing their information security systems is a top goal of the new OPM leadership, it is clear that action should have been taken years ago.

Federal computer information systems are guided by FISMA. In this risk management approach, agencies evaluate the type of data in their systems, determine what level of controls are needed, and put together a plan to adequately protect their data.

Although NIST is responsible for drafting the standards used by the agencies, they do not oversee the program and are not responsible for enforcing agency compliance with FISMA.

Instead of picking on one federal agency, it is my hope that we can use this data breach as a starting point for addressing federal cybersecurity more broadly. What is working? What is not? What mechanisms need to be in place to better protect individuals' personal information on our federal systems?

I want to end by saying that any conversation about federal cybersecurity must include a discussion about resources. It would be irresponsible for us to mandate additional cybersecurity measures that federal agencies must take without providing them with additional resources.

Cybersecurity will always be about managing risks. No information security system, whether public sector or private sector, can be completely protected. And unfortunately the question is, when, not if a system will get hacked. Therefore, we must ensure that we have the appropriate

policies and oversight in place to help federal agencies protect their data, and that we have provided federal agencies with the resources they need to do the job effectively.

I want to thank the witnesses for their testimony and I yield back the balance of my time.