OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
"Evaluating FDIC's Response to Major Data Breaches:
Is the FDIC Safeguarding Consumers' Banking Information?"
July 14, 2016

Thank you Mr. Chairman.

As we have learned over the course of many hearings before this Committee, cybersecurity is a never ending struggle. Public and private entities alike are engaged in a constantly evolving challenge to prevent both intentional data breaches and unintentional dissemination of sensitive information. Since the last hearing we held on data breaches at the Federal Deposit Insurance Corporation (FDIC), just two months ago, 32 million Twitter users had their login credentials compromised, Walmart's corporate headquarters disclosed the unauthorized access to data of more than 27,000 customers, and the medical records of thousands of National Football League (NFL) players were compromised when a laptop computer was stolen from a car.

Today is the Committee's second hearing on the FDIC's handling of several data breaches that occurred since October 2015 when the Office of Management and Budget (OMB) issued new cybersecurity guidance. The OMB memo, known as Memo 16-03, helped to define what constitutes a "major" data breach and requires reporting incidents designated as major to Congress within seven (7) days of such a determination. Data from the FDIC is particularly sensitive, and may include personal banking information and data indicating potential criminal activity, known as Suspicious Activity Reports.

The Agency failed to notify Congress of seven major data breaches within the seven-day timeframe that OMB requires from October 2015 through February 2016. During our Oversight Subcommittee hearing on this topic in May, the FDIC's Chief Information Officer (CIO), described these data breaches as "inadvertent" and occurring without "malicious intent." The FDIC Acting Inspector General Mr. Fred Gibson testified at that hearing and is a witness again today. His office released two audits of the FDIC's data breaches last week and the evidence his office gathered clearly shows that in at least one of the seven breaches the data was not taken accidentally. His office is in the process of conducting a further forensic review of the remaining 6 incidents.

I think it's fair to say that our May hearing yielded bipartisan agreement that the FDIC's interpretation of the OMB guidance was flawed. It is also clear that FDIC did not initially provide all documents responsive to the Committee's requests. However, I do not agree with my Majority colleagues as to what constitutes evidence of intent. The Majority is likely to allege that the CIO intentionally mislead this Committee and that the Agency attempted to obstruct the Committee's investigation into these events. I do not believe the Committee has uncovered convincing evidence to support those allegations. I am not dismissing the testimony of some of the FDIC employees who have been interviewed. But it is our responsibility to make sure we have all of the evidence and have heard from all parties before we begin to wave around serious allegations of criminal intent.

What I do believe is this:

First, the recent reports issued by the Inspector General's office on the data breaches at FDIC point to a series of corrective actions that I hope will improve the agency's ability to appropriately respond to the multiple cybersecurity threats we all face. I do believe the FDIC Chairman takes these issues seriously. He has a strong track record on responding to cybersecurity challenges, including holding his staff accountable.

Second, all federal agencies need a strong, competent and independent Chief Information Security Officer, and I am glad that both the IG's office as well as the Government Accountability Office (GAO) are now engaged in separate reviews about the appropriate role, placement, and authorities of the Chief Information Security Officer at FDIC and other federal agencies.

And finally, while we investigate failures at different agencies to fully and properly implement federal cybersecurity requirements, we should also support agency efforts to continue to strengthen their cybersecurity posture as the technologies and threats rapidly evolve around them.

I look forward to hearing from both Chairman Gruenberg and Acting IG Mr. Gibson.

I yield back.