OPENING STATEMENT

Ranking Member Eddie Bernice Johnson (D-TX)

House Committee on Science, Space, and Technology
Subcommittee on Oversight
"FDIC Data Breaches:
Can Americans Trust that Their Private Banking Information Is Secure?"
May 12, 2016

Thank you Chairman Loudermilk, and thank you to our two witnesses for being here today.

All data breaches that expose sensitive personal information should be taken very seriously. In today's digital age our sensitive personal data is everywhere. When we swipe our credit cards at the grocery store, renew our drivers' licenses at the Department of Motor Vehicles and passports at the Department of State, or visit the emergency room at the local hospital or the bank around the corner, our sensitive personal and financial data is processed, stored and entrusted to those entities to safeguard it and ensure it is not inadvertently breached or intentionally stolen.

But that has happened seven times in the past seven months in major cyber breaches at the Federal Deposit Insurance Corporation (FDIC). None of these breaches were the result of sophisticated hackers, foreign adversaries or cyber criminals. And those that downloaded this data, including Social Security Numbers and Suspicious Activity Reports (SARs) did not use high-tech digital tools. They simply plugged in thumb drives and other removable media to their FDIC workstations in the office and downloaded sensitive personal and financial data onto their personal storage devices jeopardized the data security of thousands of individuals, multiple banks and potentially criminal investigations.

In virtually each of these seven instances, the FDIC has said the sensitive data was inadvertently downloaded and that there was no malicious intent. I hope that that is true, but I fear that it is not. In all of these cases the FDIC was able to recover the data, and the former FDIC employees signed affidavits saying they had not shared the data with others.

However, in at least one case, according to the FDIC's own records, a former employee who downloaded such data, was evasive about her actions and not cooperative when initially confronted by FDIC staff. Some FDIC employees also suggest it was highly improbable this former employee's actions were accidental. In addition, this former employee is now working for a U.S. subsidiary of an Indian financial services company, which raises additional concerns.

I would remind FDIC that in 2013 an Inspector General review of another, much more serious, cyber incident at the Agency resulted in one senior official in the CIO's office leaving the Agency and another being demoted. My understanding is that this was not due to FDIC's response to this threat, but the lack of candor by the former officials in the CIO's office in describing the extent of this penetration and the consequences to the Agency to both the Chairman of the FDIC, the IG's office and the Government Accountability Office (GAO).

I hope the IG's office will be able to clarify whether or not all of the recent data breaches were "inadvertent," as FDIC has claimed, or not, when his office completes the two audits they are currently working on regarding FDIC's handling of "major" cybersecurity incidents in the coming weeks. I also hope the IG's office can shed some light on the reasons why the office of the Chief Information Officer (CIO) and the FDIC failed to inform Congress of these major incidents within the seven-day timeframe required by new guidance from the Office of Management and Budget (OMB).

I believe the FDIC has already taken some positive steps in responding to the recent data breaches, phasing out the use of removable media, for instance. I encourage them to continue to ensure that sensitive data is not intentionally or inadvertently breached. But I would also advise the new CIO, Lawrence Gross, testifying before us today, to keep Congress appropriately and fully informed, in a timely manner, when "major" cybersecurity incidents do occur.

Thank you. I yield back.