

OPENING STATEMENT
Ranking Member Don Beyer (D-VA)
of the Subcommittee on Oversight

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.

Defending against cyber threats is a persistent and evolving battle. The cyber hazards that confront the public and private sectors come in various forms. Hackers can and have wreaked havoc on Hollywood studios, global financial institutions, retail outlets, and public agencies alike. No one seems to be immune from the various cyber threats that touch virtually everyone.

In the case of the Federal Deposit Insurance Corporation, or FDIC, they have suffered from seven “major” cyber incidents in the past seven months. These breaches involved plugging “removable media,” such as an USB drive, into an FDIC computer and removing thousands of sensitive financial and other records from the Agency as employees walked out the door. We will be focusing on two of these breaches today as well as the FDIC’s cybersecurity practices.

I am glad that FDIC recently installed new software that allowed them to identify these recent breaches and respond to them. Without that technology, known as a Data Loss Prevention (DLP) tool, these incidents, whether inadvertent or intentional, would have gone unnoticed and unaddressed, and Congress would have remained uninformed. I also believe the FDIC Chairman has taken some positive steps in the wake of these breaches, phasing out the use of removable media, such as flash drives and CDs, for instance, that pose increased security risks.

However, I do have questions about why there was such a long delay in notifying Congress about “major” cyber incidents, particularly the one that occurred last October and was not reported to Congress until February 26, 2016. In that instance, it took a Memo from the FDIC Inspector General’s office to the FDIC CIO reminding the Agency that they had an obligation to report the incident to Congress. I would add that the IG was not the only one suggesting that the FDIC notify Congress of the incident. It is my understanding that other FDIC employees had also recommended reporting this incident to Congress months earlier.

In addition, I believe the new OMB guidance on “Federal Information Security and Privacy Management Requirements,” as detailed in OMB Memo 16-03 last October, is very clear. If it takes eight hours or more to recover sensitive data that comprises 10,000 or more records or affects 10,000 or more people it is considered a “major” cyber incident. Under these guidelines, once an Agency is aware that a breach meets that criteria, the incident should be considered a “major” breach and must be reported to Congress within seven calendar days.

That did not happen in either of the two cases this hearing will focus on, or the five others that the FDIC just reported to the Committee this week, and I am still unclear why. In the October incident the breach included records from eight banks, more than 40,000 individuals and 30,000 entities, including sensitive Bank Currency Transaction Reports and Social Security Numbers. Despite the OMB requirement that Agencies inform Congress of 'major' incidents within seven days, FDIC notified Congress nearly three months after it had enough data to determine that this was a 'major' breach.

I hope that Mr. Gross, the Chief Information Officer (CIO) at FDIC, who is testifying today can help explain FDIC's decision to delay notifying Congress in that October incident. I also hope he can help us understand the Agency's characterization of this incident, which appears to be at odds with some of the information obtained by the Committee. I know the Inspector General has looked at the October incident and the FDIC's response to it, and I am looking forward to IG Gibson's testimony as well.

Lastly, Mr. Gross, I understand you just arrived at FDIC in November and that the CIO's office has suffered from a lack of consistent leadership for some time. You are now the fourth CIO the FDIC has had in the past four years. I hope that you will be able to bring some stability to that office. But equally important is establishing a solid foundation built on reliability and openness with Congress. I hope that you will strive to do that as well.

Thank you to both our witnesses for being here today and I look forward to your testimony.

I yield back.