COMMITTEE ON
SCIENCE, SPACE, & TECHNOLOGY
Lamar Smith, Chairman

For Immediate Release
May 12, 2016

Media Contacts: Alicia Criscuolo, Thea McDonald
(202) 225-6371

Statement of Oversight Subcommittee Chairman Barry Loudermilk (R-Ga.)
FDIC Data Breaches: Can Americans Trust that Their Private Banking Information is Secure?

Chairman Loudermilk: Good morning. We are here today to learn more about cybersecurity breaches at the Federal Deposit Insurance Corporation (FDIC). As a former software company owner for over 20 years, I know first-hand the importance of safeguarding sensitive information and private customer data. Regrettably, the American people have good reason to question whether their private banking information is properly secured by the FDIC.

The FDIC is an independent agency established by Congress, with the mission "to maintain stability and public confidence in the nation's financial system." Unfortunately, the FDIC is failing to live up to its mission of maintaining public confidence in the nation's financial system because the agency is failing to safeguard private banking information for millions of Americans who rely on FDIC.

During the Committee's current investigation, it has become clear that FDIC has a long history of cybersecurity incidents. According to information obtained by the Committee, in 2011, a foreign government hacked into the workstations of the former FDIC Chairman and other senior officials. It appears that this entity had access to senior officials' workstations for at least one year before the FDIC took remedial action.

More recently, in letters dated February 26, 2016, and March 18, 2016, FDIC notified the Science Committee of two major security incidents. This notification to the Committee was required in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget guidelines that require Executive Branch departments and agencies to report "major" security incidents to Congress within seven days.

The security breach reported in FDIC's February 26th letter to the Committee involved an FDIC employee who copied sensitive personally identifiable information or PII for over 10,000 individuals onto a portable storage device prior to separating from employment at the FDIC.

The employee also downloaded "Suspicious Activity Reports, Bank Currency Transaction Reports, [Bank Secrecy Act] Customer Data Reports and a small subset of personal work and tax files. This security incident is particularly troublesome given that the FDIC did not ultimately recover the portable storage device from the former employee until nearly two months after the device was removed from FDIC premises. Further, according to information obtained by the Committee, the FDIC did not report the incident to Congress within the seven day time period as required by FISMA.

In fact, FDIC waited for over four months to report the incident to Congress and only did so after being prompted by the FDIC Office of Inspector General. Just as troubling, FDIC continues to maintain that the employee "accidently" copied sensitive and proprietary information to a portable storage device despite the fact that the employee initially told the agency that she "would never do such a thing" and even denied ever owning a portable storage device. Ultimately, she retained legal counsel who engaged in protracted negotiations with the agency for the return of the device.

The second security breach reported to the Committee on March 18, 2016, involved a disgruntled FDIC employee who obtained sensitive data for 44,000 individuals prior to separating from employment at the agency. When the employee left the FDIC on February 26, 2016, the employee took the storage device from the premises. Upon learning of the incident three days later, FDIC personnel worked to recover the device. The device was ultimately recovered on March 1, 2016. According to the FDIC, this was just another case of an employee "accidently" leaving the agency with sensitive information.

This week, FDIC retroactively reported five additional major breaches to the Committee. In one of those instances, an employee retired from FDIC and took three portable storage devices containing over 49,000 individuals' personal data. In total, over 160,000 individuals have recently been a victim of having their personal information leave the FDIC by "accident." To date, FDIC has failed to notify any of those individuals that their private information may have been compromised.

According to the FDIC, none of the 160,000 individuals has anything to worry about because all of the FDIC employees who improperly walked out of the agency with sensitive information were required to sign affidavits stating the information was not disseminated. At best, this is a misleading statement because apparently all employees who are separating from FDIC are generally required to sign an exit document attesting that they have not removed any FDIC materials from the premises. In the recent breaches reported to this Committee, all employees who improperly took the data should have already signed exit documents before ever leaving the agency.

It is Congress' responsibility to shine a light on FDIC's history of cybersecurity breaches. The Committee will continue its oversight of FDIC's failures to secure Americans' sensitive information from apparent foreign entities and disgruntled FDIC employees. I thank the witnesses for being here today and sincerely hope we are able to get answers from the FDIC here this morning. With that, I recognize the Ranking Member for his opening statement.

###