STATEMENT OF

LAWRENCE GROSS
CHIEF INFORMATION OFFICER AND CHIEF PRIVACY OFFICER
FEDERAL DEPOSIT INSURANCE CORPORATION

on

INFORMATION SECURITY

before the

SUBCOMMITTEE ON OVERSIGHT
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

May 12, 2016
2318 Rayburn House Office Building

Chairman Loudermilk, Ranking Member Beyer, and members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the important issue of cybersecurity, including our efforts to identify and address information technology (IT) security incidents. At the FDIC we are keenly aware that protecting sensitive information is critical to our mission of maintaining stability and public confidence in the nation's financial system and we are continually enhancing our information security program.

My name is Lawrence Gross and I am the FDIC's Chief Information Officer and Chief Privacy Officer. I assumed my duties at the FDIC in November 2015. As the Chief Information Officer and Chief Privacy Officer, I am responsible for providing executive leadership and oversight of the FDIC Information Technology, Privacy, Information Management, and Information Security programs. I have more than 39 years of combined military and federal sector experience in the information technology, law enforcement, cybersecurity and critical infrastructure fields. My testimony today will focus on our program to *identify, analyze, report, and remediate* incidents based on the risk of harm they pose to individuals or entities we supervise.

Identification

The FDIC has a strong information security program to *identify* events that could signal a data security incident. For example, we have mandatory annual training for all employees and contractors to ensure that they will be alert to inadequate protection of sensitive information, and know when and how to notify our Computer Security Incident Response Team (CSIRT). Employees have self-reported when they have had access to sensitive information beyond what was needed to perform their job. This is one example of a low risk incident. We also have automated monitoring tools and analysts responsible for reviewing reports from these tools on a daily basis. One example of automated monitoring is our Data Loss Prevention tool, which scans for sensitive information in outgoing emails, uploads to web sites, and any data downloaded to portable media from FDIC systems. Another tool monitors which web sites employees and contractors attempt to visit in order to prevent access to sites that may pose a risk to the agency. Our goal in the FDIC information security program is to assess and continually improve our situational awareness and shed light on events so that we can reduce and ultimately eliminate the risk of harm to individuals and entities.

Analysis

The FDIC has a security incident response and escalation plan to ensure the systematic gathering and *analyzing* of facts relevant to an event to determine the risk of harm to individuals or entities and the taking of appropriate action. When there is an elevated risk of harm, an interdisciplinary team meets to review the facts surrounding the incident and provide the CIO a recommended course of action. This team, the Data Breach Management Team (DBMT), has been in place for several years. I chair the DBMT meetings, membership on which includes representatives from the Office of the Inspector General (OIG), our Chief Risk Officer's office, the Chief Information Security Officer, our Legal Division, the division or office where the incident took place, and several others. This inter-disciplinary team works through a standardized procedure to gather facts, analyze the facts to determine the risk of harm to individuals and entities, and recommend a course of action for each incident.

Security incidents can range from situations where monitoring tools detect that a retiring employee copied sensitive information to portable media immediately prior to departing employment, to the theft of sensitive bank examination papers from an examiner's automobile, to the discovery of an external, adversarial entity attempting to breach our network defenses. In each of these cases, the incident would be reported to the Computer Security Incident Response Team (CSIRT) and, if the risk of harm is elevated, the DBMT is convened to analyze the incident. The analysis may consist of reviewing the amount and type of records potentially exposed, the circumstances surrounding the incident, and the actors involved. The DBMT asks questions and directs the gathering of additional information to gauge the risk of harm to individuals and entities in order to form a recommendation for an appropriate course of action.

Reporting

After we have gathered and analyzed the relevant incident facts, we take steps to mitigate the risk of harm, and complete the appropriate *reporting* and notifications based on the risk of harm. For example, we have had instances in the past where a thief has broken into an FDIC bank examiner's car and stolen a locked case of work papers containing bank borrower or depositor Personally Identifiable Information (PII). In those instances, the DBMT has quickly recommended notification of the individuals and the financial institutions, and the offering of credit monitoring. Another example has been when an examiner's laptop is stolen. One of the features of our information security program is that our examiner's laptop hard drives are encrypted. Since the probability of a petty thief breaking our encryption algorithm and using any PII on the laptop to cause harm is low, notifications of individuals are not typically warranted. However, all of these incidents are reported to the Department of Homeland Security's US-

CERT, to the Office of Management and Budget (OMB) in our annual Federal Information Security Management Act (FISMA) submission, and to Congress annually.

With the passage of FISMA in December 2014, and the subsequent issuance on October 30, 2015 of guidance by OMB concerning what constitutes a “major incident”, we have further refined our incident reporting regime. Notably, the new law and OMB’s guidance on “major incident” have been applied to incidents over the past six months where FDIC employees departed employment and were identified by our monitoring tools as having downloaded PII or other FDIC sensitive information to portable media not long before departure. It was my initial judgment that these incidents did not rise to the level of “major incident" as defined in the OMB guidance. I based my decision on several factors. In each case, the employee had legitimate access to the sensitive data in question while at the FDIC; our analysis indicated the downloading of the PII was inadvertent; the FDIC recovered the data from the former employees; there was no evidence that the former employee had disseminated the data; and, the former employee signed an affidavit stating they had not disseminated the data. Lastly, in each case, the circumstances surrounding the employee’s departure from FDIC employment were non-adversarial. The totality of the circumstances led to my judgment that, in each case, the former employee inadvertently downloaded the FDIC-related information while he or she was attempting to download personal files in preparation for departure. Under these circumstances, I judged the risk of harm to be very low, meaning that the reporting of these incidents would fall under the annual FISMA notification to Congress requirement.

However, our OIG reviewed one of these incidents and came to a different conclusion. The OIG, in a memorandum dated February 19, 2016, recommended that the incident they reviewed be reported to Congress under the category of "major incident". Although our interpretations differed, we nevertheless gave such notification to Congress within seven days, on February 26, 2016. In addition, I directed my staff to go back through all incidents that had occurred since October 30, 2015, on which we had already made determinations, to identify any incidents that had characteristics we thought would meet the OIG's interpretation of "major incident" and the FDIC has now reported those as well to Congress.

Remediation

Recognizing the potential risk associated with the use of portable media, we have taken additional *remedial* steps to further lower the risk of sensitive information being exposed through this channel. Several changes we are making as part of a sixty day review to lower the risks of future incidents are highlighted below.

- We have implemented a plan to eliminate the ability of employees or contractors to download to portable media (such as DVDs, CDs and flash drives). We have already implemented technology to remove the ability of the majority of employees to download any data from FDIC systems to portable media. For those members of our workforce whose business processes continue to require that they use this technology, we are actively working to identify and implement alternative means to securely exchange data with entities such as our state banking department counterparts by the end of 2016. In addition, as of Friday, May 13, software will force encryption of portable media in those instances when business processes require continued use.

- We are implementing Digital Rights Management (DRM) software to better protect our most sensitive information. The purpose of DRM is to prevent unauthorized redistribution of digital information. DRM can prevent or limit copying, and can limit the time period in which the content can be accessed, among other features. DRM technology can provide an efficient preemptive approach to the challenges of data exfiltration when compared to reactive technologies that identify issues after the fact.
- In addition to technological changes I have highlighted, I have directed my staff to begin immediately a top to bottom review of all current FDIC IT policies and procedures with a focus on revising policies and procedures for departing employees, and ensuring IT security policies associated with IT security incident management are current and incorporate recent changes in OMB guidance. This policy review and revision initiative will ensure that current and departing employees understand the policy and are aware of the requirements in downloading any data, personal or business, and we will provide them with the assistance to do so where appropriate.
- Finally, I will be engaging an independent third party to conduct an end-to-end assessment of the FDIC IT Security and Privacy Programs. The program review will encompass all key areas of the FDIC's IT security program including: network security, software security, host security, data protection, identity and access management, threat and vulnerability management, asset management, security monitoring and compliance, third party management, privacy, business continuity management, incident management, data infrastructure (i.e., events, alerts, and logs), policies and standards, awareness and training, program metrics and reporting, and governance and organization. The resulting analysis will identify any potential gaps in the FDIC's security and privacy programs and

outline a mitigation plan with measurable remediation steps required to address gaps, vulnerabilities and risks identified.

Conclusion

The global interconnected landscape continues to evolve and the threat and threat actors continue to develop tools and techniques to thwart our IT defenses. The FDIC is committed to meeting this evolving challenge by refining our operational policies and procedures on an ongoing basis to meet and mitigate the evolving threats. The FDIC takes very seriously cyber security, incident management, and transparency as it relates to our reporting requirements and remains committed to maintaining a robust IT security program that ensures a real time current view of our situational awareness. This real time view is essential to our ability to protect against and mitigate cyber related incidents proactively. That concludes my opening remarks. Thank you again for the opportunity to testify today. I would be happy to answer your questions.