Statement of
Martin J. Gruenberg, Chairman,
Federal Deposit Insurance Corporation
On
Information Security at the FDIC
Before the
Committee on Science, Space, and Technology
U.S. House of Representatives
2318 Rayburn House Office Building
July 14, 2016

Chairman Smith, Ranking Member Johnson, and members of the Committee, thank you for the opportunity to testify before you today about the important issue of information security, including our efforts to identify and address information technology security incidents.

An effective FDIC information security and privacy program is critical to our mission of maintaining stability and public confidence in the nation's financial system. My testimony today will discuss the FDIC's cybersecurity posture, recent incidents pertaining to information security, and our response to the related Office of Inspector General audits.

The FDIC's Cybersecurity Posture

The National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," dated February 12, 2014, is a product of the President's Executive Order1 calling for the development of a voluntary risk-based cybersecurity framework to serve as industry standards and best practices for managing cybersecurity risks. The framework, created through collaboration between government and the private sector, adopts a common language to address and manage cybersecurity risk, and is the framework being used by the FDIC. The framework is composed of five functions: Identify, Protect, Detect, Respond, and Recover.

1. Identify

- The "Identify" function includes understanding the organization's business context, the resources that support its critical functions, and the related cybersecurity risks. Understanding these factors enables an organization to focus and prioritize its efforts, consistent with its risk-management strategy and business needs. In carrying out the "Identify" function, the FDIC seeks to explicitly identify our assets and characteristics useful in risk-mitigation activities. Our cyber assets include hardware, software, and data. We strive to keep accurate inventories of these assets and to categorize them from a risk standpoint so that higher-risk assets receive more attention when designing cybersecurity protections. For example, we have long maintained an inventory of

our most sensitive data, including confidential bank examination reports, bank failure projections, and employees' sensitive personally identifiable information. We are currently updating that inventory and our process for maintaining it based on the Office of Management and Budget's (OMB) "high value asset" guidance.2

2. Protect

- The "Protect" function of an organization's information security posture includes developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. It speaks to an organization's ability to limit or contain the impact of a potential cybersecurity event. At the FDIC we have developed and implemented safeguards such as identity and access management, security awareness and training programs, data security protections, information protection processes and procedures, system maintenance routines, and protective technologies. In this function particularly, we strive for a "defense in depth" approach, so that if one safeguard fails, another will help us mitigate the potentially harmful impact of the failure. Our encryption of the hard drives of all of our examiners' laptops is a good example of a "Protect" activity. Also, as part of annual cybersecurity training required for all FDIC employees, we instruct our employees to be alert to anything that doesn't look right from an information security perspective ("see something/say something"). Periodic training exercises include mock email "phishing" campaigns. When an individual "fails" and clicks on an email link that should have seemed suspicious, they are immediately directed to a training page that identifies for them the email components that should have tipped them off. A final example of our activity in the "Protect" function is our recently adopted configuration of software to prevent an employee or contractor from copying information to removable media.

3. Detect

- The "Detect" function of an organization's cybersecurity posture includes developing and implementing appropriate activities to identify the occurrence of a cybersecurity event. For example, logging various system actions allows us to monitor for anomalous activity. Another example of the many tools we use under the "Detect" function is the Data Loss Prevention or "DLP" software. DLP software monitors email traffic, uploads to websites, and printing for high-risk attributes that we have specified ahead of time. We review DLP reports for indications of activity inconsistent with our policies and procedures and take additional investigative steps when the circumstances warrant.

4. Respond

- The "Respond" function of an organization's cybersecurity posture includes developing and implementing appropriate activities when a cybersecurity event is detected. For example, we have business continuity plans, which we revise

periodically, that identify the steps we would take if a cybersecurity event rendered our primary datacenter inoperable. We also practice twice a year the failover of our mission critical systems to our backup datacenter. Another example of our "Respond" function is our data breach response program. We have an internal FDIC Computer Security Incident Response Team (CSIRT) that receives inputs from many different sources regarding events that could rise to the level of a breach. The team has procedures for escalating these events based on the risk of harm indicated by the event's characteristics. When events are escalated, an interdisciplinary team is convened and follows a data breach handling guide to determine what additional analysis steps are necessary, and what risk-mitigation activities should be pursued.

5. Recover

- Finally, the "Recover" function of an organization's cybersecurity posture includes developing, implementing, and maintaining plans for restoring any capabilities or services that are impaired due to a cybersecurity event. The FDIC has disaster recovery plans that are reviewed periodically and would be followed in the event of a cybersecurity event that disabled our primary datacenter. We also practice through table top exercises what steps we would take to recover from a cybersecurity event, including the necessary communications with various counterparties and the public.

Recent Incidents and Related Audits

I would like next to address recent security incidents we experienced and two related audits by the FDIC Office of Inspector General (OIG). The first audit was of the FDIC's controls for mitigating the risk of an unauthorized release of sensitive resolution plans. The second audit was of the FDIC's process for identifying and reporting major incidents.

1. Audit of the FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans

Background

On September 29, 2015, the FDIC determined through use of its DLP software that an employee who had previously worked for the FDIC's Office of Complex Financial Institutions (OCFI) had transferred copies of sensitive resolution plans from the internal network onto an unencrypted removable storage device (or "thumb drive"). This activity violated OCFI policy, which prohibits the storage of resolution plans on removable media, and occurred immediately before the employee's resignation.

The FDIC notified the OIG of the incident on September 29, and law enforcement officials later recovered the thumb drive containing the resolution plans, as well as a non-public executive summary of a resolution plan, from the former employee. As a

result of this incident, the OIG commenced an audit, the objectives of which were to determine the factors that contributed to this security incident and to assess the adequacy of mitigating controls established following the incident.

OIG Recommendations and FDIC Responses

The OIG audit identified several weaknesses that the FDIC needed to address and made six recommendations. We concur with the OIG's findings and recommendations, and expect to complete implementation of all of our responsive actions by the end of 2016.

First, the OIG noted that an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks by the employee. The OIG also noted that the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders, including background investigations, periodic inspections of FDIC facilities to identify security concerns, employee nondisclosure agreements, a DLP tool, and programs to help employees with personal issues.

In 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by developing draft governance, policy, and procedures, and by initiating interdivisional discussions on the topic. However, as of October 2015, the insider threat program had not been implemented.

An insider threat program is a program designed to prevent, detect, and respond to threats from malicious insiders. A malicious insider is a current or former employee, contractor, or business partner who has, or had, authorized access to an organization's network, systems, or data, and has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. An insider threat program would analyze information sources to identify situations that appear to present higher risk levels so that appropriate action can be taken.

The OIG recommended that the FDIC establish an agency-wide insider threat program that is consistent with NIST-recommended practices and applicable laws, executive orders, national strategies, directives, regulations, policies, standards, and guidelines. In response, we have committed to fully implement such an insider threat program, building significantly on certain elements that are already in place. A team of executive-level staff will finalize the FDIC's insider threat program policy statement and governance structure by October 28, 2016; an insider threat working group is being established to carry out the program by October 28, 2016; and appropriate employee awareness and training efforts will be completed by December 30, 2016.

Second, the OIG noted that a key control intended to prevent the copying of sensitive resolution plans to removable media did not function properly.

The OIG recommended that the FDIC Chief Information Officer (CIO) immediately test the effectiveness of the control designed to prohibit network users from copying information to removable media to confirm that the control operates as intended. Between October 2015 and April 2016, the FDIC's Division of Information Technology coordinated tests with OCFI and others to ensure the software that prohibits copying files to removable media was working properly. While the majority of the tests were successful, some tests identified defects in limited situations. We are now installing a new software version that addresses the observed defects and plan that installation to be completed by August 26, 2016. Documentation of the test steps and the results of the test will be improved. In addition, we will develop a comprehensive test plan and use it to regularly re-evaluate the effectiveness of the software that prohibits users from copying information to removable media.

Third, the OIG recommended that the CIO coordinate with other FDIC division and office directors to revise and/or develop written policies and procedures, as appropriate, to govern the control designed to prohibit network users from copying information to removable media. In response, by the end of September the CIO organization will coordinate with division and office directors to identify and update relevant directives and procedures to ensure consistency with the FDIC's general decision to prohibit any copying of information to removable media. This will include protocols for managing any limited exceptions to the general prohibition and a requirement for regular testing of the software control's effectiveness.

Fourth, the OIG recommended that the Director of OCFI assign a dedicated information security manager (ISM) to support OCFI, given OCFI's regular handling of sensitive resolution plans. In response, OCFI will work with FDIC human resources staff to announce and by year-end fill a position for an ISM dedicated solely to OCFI.

Fifth, the OIG recommended that the Director of OCFI evaluate whether employees should continue to be allowed to store copies of sensitive resolution plans outside of the special secure OCFI system (referred to as ODM) designed for such plans. In response, OCFI is in the process of updating its policy to prohibit the practice of storing resolution plans outside of ODM (even if certain other locations may be considered secure) and to address controls on printing and downloads of resolution plans. This updating will be completed by the end of September.

Sixth, the OIG recommended that the Director of OCFI develop appropriate policies and procedures addressing the new and enhanced security controls that had been established by OCFI following the incident in question and periodically assess the effectiveness of such controls. In response, OCFI is in the process of revising its policies and procedures to address the new and enhanced security controls, and plans to complete that work by the end of September. Particularly, OCFI will develop comprehensive procedures incorporating control activities to mitigate program risks and ensure that resolution plans are adequately safeguarded, including plans for periodic testing to ensure that the controls are repeatable, consistent, disciplined, and operating as intended.

In summary, the FDIC controls intended to protect resolution plans did not work with regard to the incident in question. This is a serious matter that must be addressed so that it does not happen again. The OIG's review has been helpful to us in identifying the necessary corrective actions, and we will diligently complete them.

The second audit I would like to address is the OIG's Audit of the FDIC's Process for Identifying and Reporting Major Incidents.

Audit of the FDIC's Process for Identifying and Reporting Major Incidents

Background

This audit stemmed from a breach of sensitive information that is referenced in the OIG report as the "Florida Incident." This incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information of bank customers, to removable media. The employee took the information when the employee left the FDIC on October 15, 2015. The FDIC detected the incident through its DLP software on October 23 and notified the CSIRT. The individual's former supervisor initially contacted the individual on October 26, 2015. On November 2, 2015, the current Chief Information Officer arrived at the FDIC. On November 6, the FDIC requested assistance from the OIG's Office of Investigations (OI) to resolve the incident and OIG initiated a request that same day for additional information. On November 19, 2015, and December 2, 2015, the FDIC again had contact with the employee who was initially resistant but ultimately returned the device on December 8, 2015.

Also during this time period, on October 30, 2015, OMB issued its Memorandum M-16-03, which provides federal agencies with guidance on the reporting of "major incidents." Although OMB Memorandum M-16-03 was received after the incident occurred, the guidance nonetheless was considered and applied as part of the FDIC's ongoing response to the incident. In initially assessing the application of this new guidance, and consistent with existing FDIC policy and procedure, the CIO considered the incident's risk of harm and reached the conclusion that although it was a breach, it did not rise to the level of a "major incident."

On February 19, 2016, the FDIC received an OIG memorandum containing analysis of the Florida Incident in which the OIG concluded that the FDIC had not properly applied the OMB guidance for classifying the incident as a "major incident."3 The OIG found that the FDIC had based its determination that the Florida Incident was not a major incident on various mitigating factors related to "risk of harm" posed by the incident, but that such factors are not addressed in M-16-03 and therefore are not relevant in determining whether incidents are major. The OIG determined that the FDIC should instead have reported the Florida Incident to Congress as a major incident no later than seven days after it was determined that more than 10,000 unique Social Security numbers were involved in the breach.

We received this OIG memorandum regarding congressional notification on February 19, 2016, while the OIG's audit was still ongoing. We then proceeded to give such notification on February 26, 2016. We also reviewed other incidents that had occurred since issuance of M-16-03 and reported six additional incidents to Congress between March and May 2016.

The OIG also concluded that when the FDIC notified Congress of this incident, the notifications were inadequate. Particularly, the OIG stated that the notifications did not accurately portray the extent of risk associated with the Florida Incident.

In retrospect, and in light of the OIG's report findings, we should not have considered what we believed to be mitigating factors when applying the OMB guidelines. Having carefully reviewed the OIG audit, we agree with the OIG's conclusions and are working on each of the recommended corrective actions, as outlined below.

OIG Recommendations and FDIC Responses

The OIG final audit stemming from the Florida Incident identified several weaknesses that the FDIC needed to address and made five recommendations. We concur with the OIG's findings and recommendations and expect to complete implementation of all of our responsive actions by the end of 2016.

First, the OIG report notes that FDIC incident response policies, procedures, and guidelines did not address major incidents and recommends that the CIO revise the FDIC's incident response policies, procedures, and guidelines to address major incidents. In response, we are revising our incident response policies and other relevant documents as indicated. The CIO has already issued an interim update of our Data Breach Handling Guide to explicitly refer the reader to FISMA and M-16-03 as the operative guidelines for what constitutes a major incident for congressional reporting purposes. Further, a more comprehensive review and revision process is underway with respect to the Data Breach Handling Guide and other relevant FDIC policy and procedure documents to refine roles and responsibilities for designating incidents appropriately and to ensure incidents are appropriately escalated for action, including timeliness of decision-making and congressional notification. This comprehensive review and revision will be completed by the end of September 2016.

Second, the OIG report notes that the FDIC's DLP tool can be better leveraged to identify major incidents. The OIG recommended that the CIO review our current implementation to determine how the tool can be better leveraged to safeguard sensitive FDIC information. We agree and will review its current implementation by year-end. We will consider data classification standards guidance in assessing DLP tool keywords and filters, and will follow a project plan that identifies approved tasks resulting from the DLP review.

Third, the OIG report notes that the FDIC did not properly apply OMB guidelines in its evaluation and reporting of the Florida Incident. The OIG recommends that the CIO

ensure that revisions to the FDIC's incident response policies and procedures include criteria for determining whether an incident is major, consistent with FISMA and M-16-03.

It is important that any determination of whether an incident is major be made consistent with FISMA and M-16-03. As noted above, we have published an interim update to our Data Breach Handling Guide that directs the reader to FISMA and M-16-03 to consider when external incident notification steps are required. We will further edit policies and procedures to ensure that they are clear with respect to the criteria that should be applied for determining when an incident is major, consistent with FISMA and with M-16-03, by September 30, 2016. To ensure ongoing consistency between FDIC policy and procedure and OMB guidance, we will also review FDIC policies and procedures periodically in light of any relevant OMB revisions or other guidance obtained from OMB.

Fourth, the OIG report notes that the FDIC congressional notifications did not accurately portray the extent of risk associated with the Florida Incident. The OIG recommended that the CIO establish controls to ensure that future congressional notifications of major incidents include appropriate context regarding risks associated with such incidents and that statements of risk are supported by sufficient, appropriate evidence.

It is important that FDIC congressional notifications of major incidents include appropriate context regarding the risks associated with the incidents. In response, the CIO has already issued a memorandum to his staff implementing this recommendation. The memo stresses the importance of including appropriate context in any notifications of major incidents, including the supportability of any statements of risk. The issue of appropriate context will also be taken into account in our other reviews of policies and procedures being undertaken in response to the OIG's two audits.

Fifth, as the OIG report notes, management of incident investigative records and related documentation needs improvement. The OIG recommended that the CIO review and update, as appropriate, incident response policies, procedures, and guidelines to require proper recording and central maintenance of documentation relating to investigations and decision-making.

We agree that incident documentation should be managed centrally; that it should be kept current, accurate, and complete; and that it should contain the underlying analysis for key decisions and discussions. Our review and updating of various policies and procedures as referred to previously will take these points into account and will be completed by the end of September.

As a final note with respect to both audits, it is worth noting that the FDIC has discontinued individuals' ability to copy information to removable media such as external hard drives, flash drives, and CDs or DVDs to prevent these types of incidents from occurring in the future. Exceptions are currently limited to on-site Government

Accountability Office employees, OIG staff, and a few FDIC legal technical staff as necessary for litigation, FOIA, or congressional requests that may necessitate removable media usage.

Conclusion

As I indicated at the outset, information security is critical to the FDIC's ability to carry out its mission of maintaining stability and public confidence in the nation's financial system. Our expectation is that by taking the steps outlined we will be effective in significantly minimizing the potential for similar incidents going forward. I would note that the OIG's final reports state that our planned actions are responsive to the recommendations and the recommendations are resolved. We will keep the OIG and Congress informed of our progress.

Thank you again for the opportunity to testify today. I would be happy to answer your questions.

1 Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.

2 Office of Management and Budget M-16-04.

3 OMB M-16-03.

Last Updated 7/14/2016