Testimony

Before the Committee on Science, Space,
and Technology
U.S. House of Representatives

The Federal Deposit Insurance Corporation's Information Security Posture

Statement of Fred W. Gibson, Jr.
Acting Inspector General
Federal Deposit Insurance Corporation

July 14, 2016

Statement of Fred W. Gibson, Jr.
Acting Inspector General, Federal Deposit Insurance Corporation
July 14, 2016

Chairman Smith, Ranking Member Johnson, and Members of the Committee,

Thank you for the invitation to speak with the Committee today. Since I last testified before this Committee's Subcommittee on Oversight, my office has completed two audits relevant to the information security posture of the FDIC that are now publicly available, and we are conducting additional work related to the FDIC's information security program controls, including incident handling.

MAJOR SECURITY INCIDENTS

Our first audit dealt with the FDIC's process for identifying and reporting major information security incidents and focused on one such incident (referred to as the Florida Incident). This incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information, to removable media and took this information when the employee departed the FDIC's employment in October 2015. The FDIC detected the incident through its Data Loss Prevention tool.

We determined that although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. Specifically, we found that:

- The FDIC's policies, procedures, and guidelines did not address major incidents.
- The FDIC's Data Loss Prevention tool and related processes could be better leveraged to identify major incidents.
- The FDIC did not properly apply Office of Management and Budget (OMB) guidance in Memorandum M-16-03 when evaluating the Florida Incident.
- Congressional notification letters related to the Florida Incident included risk mitigation factors that were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident.
- Key decisions pertaining to the Florida Incident were untimely, and a required notification to another federal agency was not made.
- Management of investigative records and related documentation needed improvement.

We made five recommendations intended to provide the FDIC with greater assurance that major incidents are identified and reported consistent with the Federal Information Security Modernization Act of 2014 and OMB guidance. FDIC management concurred with all five recommendations and is taking responsive actions.

The results of our analysis of the Florida Incident prompted the FDIC's Chief Information Officer to initiate a review of similarly-situated incidents that occurred after the OMB issued Memorandum M-16-03 to determine whether additional incidents warranted designation as major. The FDIC reported six additional incidents to the Congress as major between March and May 2016. We are currently conducting a review of the six incidents and the manner in which they were reported to the Congress and expect to complete this work by mid-September.

SENSITIVE RESOLUTION PLANS

In a second audit, we reviewed the Corporation's controls for mitigating the risk of an unauthorized release of sensitive resolution plans.

Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, certain financial companies designated as systemically important must report to the FDIC on their plans for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure. These resolution plans or living wills contain some of the most sensitive information that the FDIC maintains. Safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

In September 2015, an FDIC employee working in the FDIC's Office of Complex Financial Institutions abruptly resigned from the Corporation and took copies of sensitive components of resolution plans without authorization and in violation of FDIC policy. This incident is not one of the seven that the FDIC reported as major to the Congress.

Our work identified a number of factors contributing to this security incident. Most notably:

- An insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee.
- A key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended.

The remaining factors involved OCFI employees having access to resolution plans that exceeded business needs; OCFI's inability to effectively review and revoke employee access to resolution plans because employees were allowed to store copies of the plans outside of the FDIC's official system of record—OCFI Documentum (ODM); and OCFI's inability to monitor all downloading of resolution plans stored in ODM.

Our report contains six recommendations. Specifically, we recommended that the FDIC establish a corporate-wide insider threat program. The remaining five recommendations are intended to strengthen the FDIC's information security controls, particularly with respect to safeguarding sensitive resolution plans submitted to the Corporation under the Dodd-Frank Act.

The FDIC has outlined actions that are responsive to the recommendations in our report, and we will follow up on the implementation of those recommendations, as appropriate.

ONGOING WORK

In addition to our ongoing work with regard to the six reported incidents, we will complete this year's FISMA audit in the fall. The report will build upon the work I have described today and will broadly assess the effectiveness of the FDIC's information security program and practices. In addition, we have ongoing work related to the FDIC's plans and actions to address prior recommendations that we made pertaining to credentialing and multifactor authentication. We plan to initiate additional work in such areas as data breach notifications and the FDIC's information technology enterprise architecture.

Finally, we also have open criminal investigations relating to several of the incidents, which have not reached a stage where further public discussion would be appropriate.

Thank you, again. I look forward to answering any questions the Committee may have about these or related matters.