Office of Inspector General

Executive Summary

The FDIC's Controls for Safeguarding Sensitive Information in Resolution Plans Submitted Under the Dodd-Frank Act

Report No. AUD-14-008
July 2014

Why We Did The Audit

Section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act) and the FDIC and Board of Governors of the Federal Reserve System's (FRB) Final Rule, entitled *Resolution Plans Required*, dated November 1, 2011, require large, systemically important financial companies to submit resolution plans, sometimes referred to as "living wills," to the FDIC and to the FRB. The intent of this requirement is for a large financial company to describe how it could be resolved under the U.S. Bankruptcy Code without serious adverse effects on U.S. financial stability. The resolution plans required by section 165(d) and the Final Rule contain sensitive information. Accordingly, safeguarding the plans from unauthorized access or disclosure is critical to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

The audit objective was to determine whether the FDIC's controls for safeguarding sensitive information in resolution plans submitted under section 165(d) of the Dodd-Frank Act are consistent with applicable information security requirements, policies, and guidelines. We conducted the audit in two phases. During the first phase, we assessed the FDIC's controls over sensitive resolution plan information and briefed FDIC management in February 2013 on our preliminary observations. During the second phase, we determined the status of actions that had been taken to address our preliminary observations as of February 2014.

Background

The Final Rule established a staggered schedule for submitting resolution plans based on the amount of total nonbank assets that financial companies own. The first group of filers consisted of 11 companies with $250 billion or more in non-bank assets. Nine of these companies submitted initial resolution plans by July 1, 2012, and the remaining two companies submitted initial plans by October 1, 2012. Our audit focused on the controls that the FDIC had in place to safeguard resolution plans submitted by this first group of financial company filers.

The FDIC and FRB jointly review the resolution plans to determine whether they would facilitate an orderly resolution of the company under the U.S. Bankruptcy Code. Within the FDIC, the Office of Complex Financial Institutions (OCFI) has primary responsibility for reviewing the resolution plans submitted by the first group of financial company filers. The results of the FDIC's reviews, including findings and analyses, are contained in electronic and hard-copy documents referred to as Review Materials. The FDIC has determined that Review Materials constitute sensitive information.

Information security requirements, policies, and guidelines applicable to safeguarding sensitive information in resolution plans include relevant provisions of the Dodd-Frank Act and the Federal Information Security Management Act of 2002, National Institute of Standards and Technology security standards and guidelines, the Government Accountability Office's *Standards for Internal Control in the Federal Government*, Office of Management and Budget guidance, and FDIC policies and procedures.

Audit Results

We initially found that the FDIC's controls for safeguarding sensitive information in resolution plans submitted under section 165(d) of the Dodd-Frank Act were not fully consistent with applicable information security requirements, policies, and guidelines. Among other things, we found that the

security level of sensitive resolution plan information had not been formally categorized in accordance with federal standards, key OCFI security policies and procedures needed to be updated and finalized, access controls needed to be strengthened, and the role and level of resources allocated to OCFI's internal review and information security functions needed to be assessed.

We met with the Director, OCFI, in February 2013 and shared our preliminary observations from the first phase of the audit. We also met with officials in the Division of Administration and Division of Information Technology, which began reporting to the newly appointed Chief Information Officer (CIO) in July 2013, because these officials had responsibility for addressing some of our preliminary observations. Throughout 2013, and prior to the close of the audit in February 2014, the FDIC was taking actions to address our preliminary observations and strengthen security controls over sensitive resolution plan information. Of particular note, the FDIC:

- formally categorized sensitive resolution plan information, including Review Materials, consistent with federal standards;
- assigned an Information Security Manager from another FDIC division to help establish and implement security controls over sensitive information maintained by OCFI;
- updated and formally approved key OCFI security policies and procedures;
- strengthened controls over the management of hard-copy resolution plans and Review Materials;
- began requiring security guards to use individual access codes when entering secured workspaces where resolution plans and Review Materials are stored to promote accountability; and
- developed a formal internal review manual and plan that address information security.

The actions taken by the FDIC since the start of the audit significantly improved the state of security over sensitive resolution plan information. Our report describes additional steps that the FDIC can take to further mitigate risk in this area. In general, these steps involve enhancing controls related to access management, encryption and authentication, internal control reviews, and personnel suitability.

Recommendations and Corporation Comments

Our report contains four recommendations addressed to the Director, OCFI, and three recommendations to the Acting CIO that are intended to enhance security controls over sensitive resolution plan information. In many cases, the FDIC was already working to enhance security controls in these areas during the audit. We identified certain other matters that we did not consider significant in the context of the audit objective, and we communicated those separately to appropriate FDIC management officials.

The Director, OCFI, and the Acting CIO provided separate written responses, dated June 20, 2014, to a draft of this report. In their responses, the officials concurred with all seven of the report's recommendations and described ongoing and planned actions that address the recommendations.

Because this report contains sensitive information, we do not intend to make the report available to the public in its entirety. We will, however, post this Executive Summary on our public Web site.