FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG
CHAIRMAN

February 21, 2016

Honorable Gene L. Dodaro
Comptroller General of the United States
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Comptroller General:

In accordance with Title III of the Electronic Government Act, I am pleased to transmit reports from the Federal Deposit Insurance Corporation and the FDIC's Office of Inspector General resulting from the Federal Information Security Management Act's annual information security program self-assessment and independent evaluation.

Your continuing support is appreciated. If you have further questions or comments, please contact me at (202) 898-3888 or Andy Jiminez, Director of the Office of Legislative Affairs, at (202) 898-7055.

Sincerely,

(b)(6) [redacted]

Martin J. Gruenberg

Enclosures

Page 2

FEDERAL DEPOSIT INSURANCE CORPORATION, Washington, DC 20429

MARTIN J. GRUENBERG
CHAIRMAN

November 13, 2015

Honorable Shaun Donovan
Director
Office of Management and Budget
Eisenhower Executive Office Building, Room 252
Washington, D.C. 20503

Dear Mr. Donovan:

Attached are reports from the Federal Deposit Insurance Corporation Chief Information Officer (CIO) and Inspector General (IG), resulting from the Federal Information Security Modernization Act's (FISMA's) annual information security program self-assessment and independent evaluation. Also attached is a report from the FDIC Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) describing the status of FDIC's privacy program. The reports were prepared following the guidance in OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*. Also included are progress reports for eliminating the unnecessary use of Social Security numbers and reducing the holdings of personally identifiable information, the FDIC's breach notification policy, and a description of the FDIC's privacy program and training. These reports are being submitted through CyberScope, the automated reporting tool for FISMA.

The FDIC has a well-established information security program that continues to progress and evolve to meet new challenges. For example, for many years the FDIC has encrypted portable devices, scanned hardware for common vulnerabilities and exposures, used two-factor authentication for remote access, and provided security awareness training to users. More recently, the FDIC has increased the frequency of awareness training on phishing and improved its security metrics reporting, which facilitates proactive management and awareness of the FDIC's security posture.

In the OIG's report entitled *Audit of the FDIC's Information Security Program – 2015*, the auditors concluded that, with some exceptions, "the FDIC's information security program and practices were generally effective." The auditors noted that management attention was warranted in security control areas such as risk management and configuration management. In its response to the report, FDIC management concurred with all six of the report's recommendations and described ongoing and planned corrective actions that were responsive.

The FDIC reported 466 incidents to the United States Computer Emergency Readiness Team (US-CERT) from October 1, 2014 to September 30, 2015. Most of these (approximately 54 percent) were category four, "Improper Usage" incidents and involved employee activities such as failing to encrypt e-mail messages containing potentially sensitive information. The table below provides a breakdown of the activity by category.

| US-CERT Category | Number of Incidents |
|---|---|
| 1 - Unauthorized Access | 159 |
| 2 - Denial of Service | 0 |
| 3 - Malicious Code | 35 |
| 4 - Improper Usage | 250 |
| 5 - Scans/Probes/Attempted Access | 1 |
| 6 – Investigation | 21 |
| Total | 466 |

These incidents involved U.S.-based systems, had limited impact, and are addressed. The CIO's report section 9, Incident Response, and the SAOP's report section 12, Breach Response and Notification, contain additional information about incidents that resulted in a breach.

The FDIC continues to improve information security consistent with CAP goals and key FISMA metrics. For example:

- All of the FDIC's endpoints belong to systems with a valid Authorization to Operate (ATO);
- All of the FDIC's public facing systems have a valid ATO;
- All of the FDIC's hardware assets connected to the network are scanned for vulnerabilities using credentialed scans with Security Content Automation Protocol-validated tools;
- All incoming e-mails are scanned using a reputation filter tool to perform threat assessment of the e-mail sender;
- All inbound network traffic passes through a web content filter that provides anti-phishing, anti-malware, and blocking of malicious websites;
- All outbound communication traffic is checked at the external boundaries to detect covert exfiltration of information;
- All remote access connections utilize Federal Information Processing Standards (FIPS) 140-2-validated cryptographic modules; and
- All remote access connections time-out within 30 minutes of inactivity.

Nevertheless, there are other areas where the FDIC needs to improve security. For example, the FDIC needs to expand secure baseline configurations to include additional software products and to continue our roll out of two-factor authentication to include non-privileged users. Initiatives in both of these areas are underway.

The FDIC also has a well-established privacy program that maintains a culture of privacy consideration, promotes transparency and public trust, and protects the FDIC and individuals from potential harm. To mitigate privacy risks, the FDIC's privacy program staff conducts awareness and training activities, develops corporate policies, procedures and guidance, and assists divisions and offices with assessing privacy risks.

The attachments provide additional insight into the status of the FDIC's information security and privacy programs. The FDIC will continue to work aggressively to make process improvements and to secure and protect data entrusted to the agency. If you have questions or would like additional information, please contact Mr. Lawrence Gross, Jr., CIO and CPO, at (202) 898-6630.

Sincerely,

(b)(6)

[redacted]

Martin J. Gruenberg

Attachments

# FDIC
# FISMA Reporting Package
# 2015

Page 6

# Table of Contents

# Chief Information Officer

Section Report

2015
Annual FISMA
Report

## Federal Deposit Insurance Corporation

## Section 1A: System Inventory

(b)(5)

1.1 **For each FIPS 199 impact level, what is the total number of operational unclassified information systems by organization (i.e. Bureau or Sub-Department Operating Element) categorized at that level? (Organizations with fewer than 5,000 users may report as one unit.) Answer in the table below.**

[redacted]

## Section 2A: ISCM - Hardware/Software Asset Management

(b)(5)

[redacted]

2.2 [redacted]

2.3

2.4 [redacted]

2.5

Softwa

2.6 [redacted]

2.7 [redacted]

2.8 [redacted]

(b)(5)

## Section 2A: ISCM - Hardware/Software Asset Management

(b)(5)

## Section 2C: ISCM - Vulnerability and Weakness Management

2.11

2.12

2.13

2.14

Secti

Unpriv

3.1

Privileg

3.2

(b)(5)

## Section 3: Identity Credential and Access Management

3.3 [redacted]

3.4

**Internal**

3.5

3.6

**Remote**

3.7

[redacted]

3.8

[redacted]

**Physical Access Control Systems**

Page 12

(b)(5)

## Section 3: Identity Credential and Access Management

3.9

3.10

[redacted]

## Sectio

4.1

4.2

4.3

4.4

4.5

4.6

4.7 Percent (%) of incoming emails scanned using a reputation filter tool to perform threat assessment of email sender.

## Section 4: Anti-Phishing and Malware Defense

(b)(5)

4.8

4.9

4.10

4.11

4.12

4.13

4.14

[redacted]

## Section 5: Data Protection

## Section 5: Data Protection

5.1

[redacted]

Sectio

6.1

Sectio

Instruct

7.1

(b)(5)

(b)(5)

## Section 7: Boundary Protection

**Questions 7.2–7.3 apply only to Federal civilian organizations. If the reporting organization is not a Federal civilian organization, answer N/A to these questions.**

**7.2**

**7.3**

**7.4**

**Secti**

**8.1**

**8.2**

**8.3**

[redacted]

## Section 8: Training and Education

## Sectio

9.1

9.2

9.3

(b)(5)

# Senior Agency Official For Privacy

## Section Report

2015
Annual
FISMA

## Federal Deposit Insurance Corporation

## Section 1: Information Security Systems

| | | 1a<br>Number of Federal systems that contain personal information in an identifiable form | | | 1b<br>Number of systems in 1a for which a Privacy Impact Assessment (PIA) is required under the E-Government Act | | | 1c<br>Number of systems in 1b covered by a current PIA | | | | 1d<br>Number of systems in 1a for which a System of Records Notice (SORN) is required under the Privacy Act | | | 1e<br>Number of systems in 1d for which a current SORN has been published in the Federal Register | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Agency/ Component | Submission Status | Agency Systems | Contractor Systems | Total Systems | Agency Systems | Contractor Systems | Total Systems | Agency Systems | Contractor Systems | Total Systems | % Complete | Agency Systems | Contractor Systems | Total Systems | Agency Systems | Contractor Systems | Total Systems | % Complete |
| FDIC | Submitted to Agency | 55 | 6 | 61 | 42 | 5 | 47 | 40 | 5 | 45 | 96% | 37 | 5 | 42 | 37 | 5 | 42 | 100% |
| | The number of SAOP systems reported in this section is based on the number of systems reported under the CIO section and includes federal systems only. | | | | | | | | | | | | | | | | | |
| *Agency Totals* | | 55 | 6 | 61 | 42 | 5 | 47 | 40 | 5 | 45 | 96% | 37 | 5 | 42 | 37 | 5 | 42 | 100% |

## Section 2: PIAs and SORNs

2a Provide the URL of the centrally located page on the organization web site that provides working links to organization PIAs (N/A if not applicable).

https://www.fdic.gov/about/privacy/assessments.html

2b Provide the URL of the centrally located page on the organization web site that provides working links to the published SORNs (N/A if not applicable).

https://www.fdic.gov/regulations/laws/rules/2000-4000.html

## Section 3: Senior Agency Official for Privacy (SAOP) Responsibilities

3a Can your organization demonstrate with documentation that the SAOP participates in all organization information privacy compliance activities?

Yes

3b Can your organization demonstrate with documentation that the SAOP participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals, as well as testimony and comments under OMB Circular A-19?

Yes

3c Can your organization demonstrate with documentation that the SAOP participates in assessing the impact of the organization's use of technology on privacy and the protection of personal information?

Yes

## Section 4: Privacy Training

4a Does your organization have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramifications of inappropriate access and disclosure?

Yes

4b Does your organization have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) that handle personal information, that are directly involved in the administration of personal information or information technology systems, or that have significant information security responsibilities?

Yes

## Section 5: PIA and Web Privacy Policies and Processes

Does the organization have a written policy or process for each of the following?

5a PIA Practices

## Section 5: PIA and Web Privacy Policies and Processes

5a(1) Determining whether a PIA is needed

Yes

5b Web Privacy Practices

5a(2) Conducting a PIA

Yes

5a(3) Evaluating changes in technology or business practices that are identified during the PIA process

Yes

5a(4) Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA

Yes

5a(5) Making PIAs available to the public as required by law and OMB policy

Yes

5a(6) Monitoring the organization's systems and practices to determine when and how PIAs should be updated

Yes

5a(7) Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained

Yes

5b(1) Determining circumstances where the organization's web-based activities warrant additional consideration of privacy implications

Yes

5b(2) Making appropriate updates and ensuring continued compliance with stated web privacy policies

Yes

5b(3) Requiring machine-readability of public-facing organization web sites (i.e., use of P3P)

Yes

## Section 6: Conduct of Mandated Reviews

Did your organization perform the following reviews as required by the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Agency Data Mining Reporting Act of 2007? Indicate “N/A” if not applicable.

| Agency/Component | a.<br>Section (m) Contracts | b.<br>Records Practices | c.<br>Routine Uses | d.<br>Exemp-tions | e.<br>Matching Programs | f.<br>Training | g.<br>Violations: Civil Action | h.<br>Violations: Remedial Action | i.<br>System of Records Notices | j.<br>(e)(3) Statement | k.<br>Privacy Impact Assessments and Updates | l.<br>Data Mining Impact Assessment |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| FDIC | Y | Y | Y | 0 | 0 | Y | Y | Y | 34 | 6 | 24 | N |
| *TOTAL* | | | | *0* | *0* | | | | *34* | *6* | 24 | |

## Section 7: Written Privacy Complaints

**Indicate the number of written complaints for each type of privacy issue received by the SAOP or others at the organization.**

**7a** **Process and Procedural — consent, collection, and appropriate notice**

**0**

**7b** **Redress — non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters**

**1**

**7c** **Operational — inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction**

**1**

**7d** **Referrals — complaints referred to another organization with jurisdiction**

**0**

## Section 8: Policy Compliance Review

**8a** **Does the organization have current documentation demonstrating review of the organization's compliance with information privacy laws, regulations, and policies?**

**Yes**

**8b** **Can the organization provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?**

**Yes**

**8c** **Does the organization use technologies that enable continuous auditing of compliance with stated privacy policies and practices?**

**Yes**

**8d** **Does the organization coordinate with the organization's Inspector General on privacy program oversight?**

**Yes**

## Section 9: SAOP Advice and Guidance

## Section 9: SAOP Advice and Guidance

**Please select "Yes" or "No" to indicate if the SAOP has provided formal written advice or guidance in each of the listed categories, and briefly describe the advice or guidance if applicable.**

**9a** **Organization policies, orders, directives, or guidance governing the organization's handling of personally identifiable information**

Yes

**9b** **Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching, and similar issues**

Yes

**9c** **The organization's practices for conducting, preparing, and releasing SORNs and PIAs**

Yes

**9d** **Reviews or feedback outside of the SORN and PIA process (e.g., formal written advice in the context of budgetary or programmatic activities or planning)**

Yes

**9e** **Privacy training (either stand-alone or included with training on related issues)**

Yes

## Section 10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking technologies")

**10a** **Does the organization use web management and customization technologies on any web site or application?**

Yes

**10b** **Does the organization annually review the use of web management and customization technologies to ensure compliance with all laws, regulations, and OMB guidance?**

Yes

**10c** **Can the organization demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies?**

Yes

**10d** **Can the organization provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies?**

Yes

## Section 10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking technologies")

(b)(5) 10e [redacted]

## Section 11: Information System Security

(b)(5) 11a

11b

[redacted]

## Section 12: Breach Response and Notification

**Pursuant to FISMA, each federal agency is required to notify and consult with US-CERT regarding information security incidents involving the information and information systems. New US-CERT Federal Incident Notification Guidelines are effective October 1, 2014.**

(b)(5) 12a

12b

12c

12d

[redacted]

FDIC FEDERAL DEPOSIT
INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Chief Information Officer Organization (CIOO)

# Information Security and Privacy Staff (ISPS)

# FDIC Continuous Monitoring Methodology

May 2015

# Revision History

| Version | Date | Revision | Changes | Author | Reviewer |
|---|---|---|---|---|---|
| Initial 1.0 | 6/30/2011 | Version 1 - Final | - Published original document | [redacted] | [redacted] |
| 2.0 | 6/30/2012 | Version 2 - Final | - Remove "Tactical Plan"<br>- Remove "Section 4: Tactical Plan..."<br>- Updated acronyms and terms | [redacted] | [redacted] |
| 3.0 | 5/19/2015 | Version 3 – Final | - Updates to reflect changes in laws and program details. | [redacted] | [redacted] |
| | | | | | |

(b)(5),(b)(6)

## Table of Contents

## Table of Figures

# 1 Executive Summary

The Federal Deposit Insurance Corporation (FDIC) maintains a comprehensive, corporate-wide Continuous Monitoring (ConMon) Program that was independently verified as an established program in a 2010 OIG audit report[1]. This document refines the FDIC's current ConMon methodology and practices.

Updates to NIST Special Publications (SP) necessitated agency reviews of their practices, policies, and procedures. Key points in the recent NIST publications detailed the need for agencies to fully implement the concepts and practices of "continuous monitoring" across organizations and refine their risk management frameworks accordingly. Such frameworks provide on-going awareness to support organizational risk decisions.

The ConMon Team documented the current continuous monitoring state and enhanced the existing program. Program enhancements transformed the process from assessing all NIST controls every three years to testing controls on a risk and frequency-based determination. Specifically, a risk-based control selection approach will promote a cost-effective information security assurance program that reduces the required resources (dollars, people, and time) needed for continuous reauthorization of FDIC's applications and systems.

[1] 2010 Annual FISMA Report by the Inspector General (OIG Report – Annual 2010)

# 2 Overview

## 2.1 Purpose

This Methodology documents the FDIC's Continuous Monitoring Program and provides details of all supporting activities. The FDIC's Continuous Monitoring Program was independently verified as an established program in a 2010 OIG audit report; this methodology document describes all Information Assurance activities required to support the Program.

This document will be reviewed annually during our FISMA reporting cycle and updated as necessary.

## 2.2 Intended Audience

The methodology is designed to be utilized by parties responsible for the management of the enterprise-wide Information Security Assurance program, as defined and updated by NIST SP 800-37, rev. 1. This includes Information Security and Privacy Staff (ISPS) staff, auditors, and managers interested in understanding the entire FDIC ConMon Program

## 2.3 Background

The Executive Office of the President and NIST have emphasized the need to continuously monitor information systems on a near real-time basis. The FDIC began an assessment of the agency's current Continuous Monitoring program to determine its alignment with NIST guidance and identify gaps between current processes and those outlined by NIST. As a result of this assessment, several artifacts were developed and used as input to the Program[2].

- The Federal Information Security Management Act (FISMA) of 2002, which was updated in 2014, requires agencies to conduct assessments of security controls as a critical step within the NIST's Risk Management Framework (RMF).
- In NIST SP 800-37, the concept is expanded to include an organization-wide perspective, integration with the system development life cycle (SDLC), and support for ongoing authorizations.[3]
- In NIST SP 800-137, defines an information security continuous monitoring program (ISCM) as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." 800-137 goes on to establish the basis for and guidance on implementing an ISCM program within a federal agency.[4]

[2] Current State of Continuous Monitoring, December 2010; Continuous Monitoring Strategic Framework, January 2011

[3] http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

[4] http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

- OMB M-10-15 (FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) requires agencies to continuously monitor security-related information from across the enterprise and utilize CyberScope for reporting.[5]
- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, requires federal agencies are required to develop and maintain an information security continuous monitoring (ISCM) strategy that "address all security controls selected and implemented by agencies, including the frequency of and degree of rigor associated with the monitoring process."[6]

ISPS formed a ConMon Team to identify the current continuous monitoring state and developed plans for improving the established program. The ConMon team conducted various research activities and reviewed all relevant NIST documents related to ConMon, including SP 800-37 rev. 1, 800-39, 800-137, and 800-128. The ConMon team conferred with other FDIC groups to leverage knowledge of existing tools and coverage of these tools to NIST controls. The Team held sessions with Divisional Internal Controls points of contacts regarding collaboration on business process-related security activities. The team held meetings with several vendors to discuss their product's coverage of NIST controls, and also met with several Federal agency representatives to understand their approach for implementing a continuous authorization process.

FDIC currently utilizes numerous security/software tools. To take full advantage of these tools, several initiatives were conducted. A tools capability analysis helped to identify the security controls that could be tested in an automated fashion and the controls that must be tested manually. The ConMon Team mapped various software tools to infrastructure components (hardware and software) and tools to NIST controls.

The Team's analysis of automated tool capabilities helped to determine the testing frequency of security controls for various components of the corporation's MAs/GSSs. The testing frequencies can be generally classified into four types: continuous, event-driven, infrequent, or not applicable.

- Continuous can be viewed as controls that are monitored periodically at some set interval (daily, weekly, monthly, quarterly, etc.) by automated tools or by manual assessment. Examples of controls that may need to be tested on a continuous basis are RA-5 (Vulnerability Scanning), SI-2 (Flaw Remediation), and SI-3 (Malicious Code Protection).
- Event-driven can be viewed as controls which can be identified under the Security Impact Analysis (SIA) process, to be evaluated as a result of a significant change. Examples of controls that may need to be tested due to a significant change event are CM-2 (Configuration Baselines), and CM-6 (Configuration Settings).
- Infrequent can be viewed as controls that are assessed on an intermittent basis, such as annually, bi-annually, etc. Examples of controls that may be "tested" on an infrequent basis are CA-6 (Security Authorizations), CA-7 (Continuous Monitoring).

[5] https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
[6] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

- Not-Applicable can be viewed as controls that FDIC has deemed unnecessary for continuous, event-driven, or infrequent monitoring. An example of N/A controls would be those that pertain to FIPS 199 rated high-baseline systems. Currently, the highest rating of any FDIC system is a FIPS 199 rating of Moderate.

Figure 1 depicts the enhanced collaboration between groups, sections, and divisions. In addition, it demonstrates FDIC's ConMon frequency model.

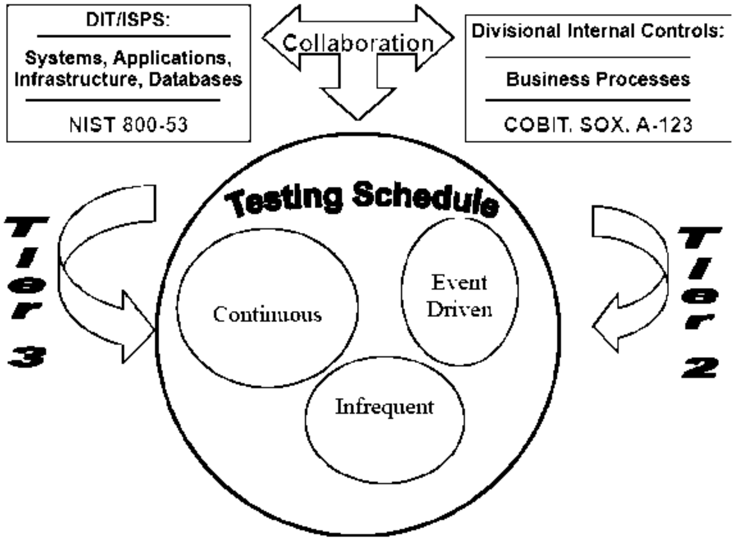


**Figure 1: ConMon Frequency Model**

# 3 Continuous Monitoring Methodology

The FDIC Continuous Monitoring Methodology is an agency-wide program that recognizes and leverages existing roles and responsibilities which support and contribute to the monitoring of FDIC's IT security risk posture.

Figure 2 illustrates a three-tiered approach to Information Security Risk Management that addresses risk-related concerns at: (i) the organization level; (ii) the mission and business process level; and (iii) the information system level.[7] It also shows FDIC related resources operating at the various tiers.

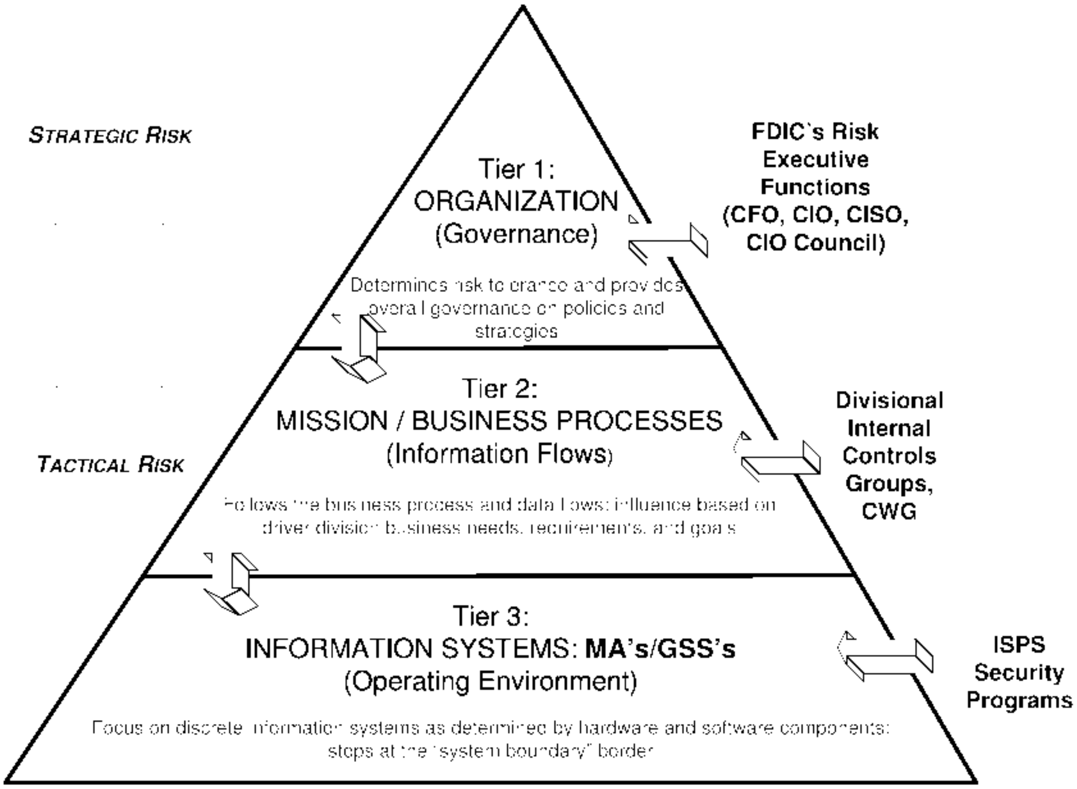

STRATEGIC RISK
TACTICAL RISK
Tier 1:
ORGANIZATION
(Governance)
Determines risk to organization and provides overall governance on policies and strategies
Tier 2:
MISSION / BUSINESS PROCESSES
(Information Flows)
Follows the business process and data flows; influence based on driven division business needs, requirements, and goals
Tier 3:
INFORMATION SYSTEMS: MA's/GSS's
(Operating Environment)
Focus on discrete information systems as determined by hardware and software components; stops at the "system boundary" border
FDIC's Risk Executive Functions (CFO, CIO, CISO, CIO Council)
Divisional Internal Controls Groups, CWG
ISPS Security Programs

**Figure 2: FDIC Tier-Mapping**

[7] http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

## 3.1 Tier-1 (Organization/Governance) Activities

The Tier-1 Organization (Governance) level contains the Risk Executive Function (REF). NIST defines the REF as “an individual or group within an organization that helps to ensure that”:

(i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and

(ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

The Tier-1 Organizational-level provides governance on FDIC’s policies and strategies and determines risk tolerance for the Corporation. FDIC has several groups within the Corporation that perform risk executive functions, including CFO, CRO, CIO, CISO, and the CIO Council to ensure governance is provided for risk-related issues. The CIO also serves as the FDIC’s Chief Privacy Officer.

## 3.2 Tier-2 (Mission/Business Process layer) Activities

In Tier-2, mission and business process activities are conducted and business processes and data/information flows are evaluated by FDIC’s divisional Internal Controls and other working groups. Below are some examples:

- Privacy Staff conduct privacy-related activities for all divisions, including physical walk-throughs to detect and remediate privacy issues, respond to privacy breaches, performs in-depth assessments, and provide consulting services and privacy awareness training.
- Agency Common Controls assessments are conducted in accordance with NIST SP 800-53A, rev 3.
- Outsourced vendor assessments are conducted on the hardware, software, and facilities of external service providers.
- Collaboration and partnerships between ISPS and divisional Internal Controls groups are being leveraged to ensure business processes contain adequate IT security controls.

## 3.3 Tier-3 (Information Systems/Operating Environment) Activities

In Tier-3, FDIC focuses testing and validating of the security controls on discrete information systems. Some of the activities in Tier-3 are listed below.

- Security Policy and Compliance Section (SPCS) conducts IT security assessments using a risk-based control selection process. A repository maintains an inventory of IT assets and maps the components to application and systems. These assets are associated to General Support Systems (GSS) and / or Major Applications (MA).

- Security Protection & Engineering Section (SPES) conducts vulnerability scanning, data loss prevention (DLP) monitoring and other assessment activities based on defined frequencies.
- Privacy staff members reviews and responds to PII and Sensitive Information data breaches.

## 3.4 Elements of Continuous Monitoring

In accordance with NIST SP 800-137, FDIC's ConMon Methodology consists of five essential processes:

- Configuration Management and Change Control
- Information Security Risk Management Program
- Security Impact Analyses (SIA)
- Security Status Monitoring and Reporting
- Active Involvement of Organizational Officials

The remainder of this section covers each of the five major tasks.

### 3.4.1 Configuration Management and Change Control

Configuration management and change control of FDIC information systems consists of documenting information system changes and assessing the risk associated with proposed changes to the security of the information system. FDIC systems undergo some level of change or migration throughout their lifecycle through, for example, upgrades to system functionality, software, and hardware.

As noted by the FDIC's Office of Inspector General (OIG), the Corporation "has established and is maintaining a security configuration management program that is generally consistent with NIST and OMB FISMA requirements"[8]. Some of attributes of the program are included below:

- Documented policies and procedures
- Standard baseline configurations
- Scanning for compliance and vulnerabilities
- Process for the timely and secure installation of software patches
- Information system component inventory

#### 3.4.1.1 Documented policies and procedures

To develop information systems, the FDIC has adopted the Rational Unified Process (RUP) as its SDLC model. The RUP process is based on a series of current best practices that include concepts such as iterative development, requirements management, risk management, and continuous verification of quality. The FDIC manages and documents all changes to information systems through the RUP process and the FDIC's change control process.

[8] 2010 Annual FISMA Report by the Inspector General (OIG Report – Annual 2010)

The Configuration Control Board (CCB) provides a formal process for reviewing and approving changes to the infrastructure and technical architecture to ensure that all changes are well planned, communicated, and coordinated. The CCB provides a mechanism to strengthen project coordination and management in the Infrastructure RUP process. The CCB has evolved in the Infrastructure RUP process as the focal point for review of Infrastructure projects in the Construction and Transition phases.

The Post Project Review (PPR) program provides the means to ensure that software related projects undertaken by or on behalf of FDIC are managed in full compliance with the RUP methodology; meet the client's expectations; meet business goals/objectives; and ensure the project management process is continuously assessed for improvement.

The Network Review Board (NRB) is a formal organization to review proposed network designs and changes not part of the pre-approved network changes list. The NRB assists the Change Control Board (CCB), and other bodies by pre-approving changes using network Subject Matter Experts (SMEs) from different organization within DIT. This allows the CCB to concentrate on scheduling concerns after approval has been granted by the NRB. The NRB will also be responsible for establishing and maintaining standards for network designs and implementation plans.

Star Team is the FDIC's repository for documenting and storing changes to hardware or software artifacts. SharePoint is the Corporation's secure workspace for collaboration on active documents and other content for business purposes.

#### 3.4.1.2 Standard baseline configurations

Configuration baselines form the foundation for secure settings for systems and applications. The Infrastructure Support Branch (ISB) is responsible for maintaining configuration baselines for IT Infrastructure components while ISPS is responsible for establishing the security requirements portion of these baselines. Baselines can be developed using NIST, CIS, DISA or vendor-provided checklists which are tailored for the FDIC environment. Deviations from FDIC baselines are documented in the System Security Plan and/or other documentation.

#### 3.4.1.3 Scanning for compliance and vulnerabilities

The SPES team uses security validation products and a security configuration management scanning solution which are defined in their internal standard operating procedures (SOPs). The two key areas are scanning for compliance and scanning for vulnerabilities.

#### 3.4.1.4 Process for the timely and secure installation of software patches

Currently FDIC use Microsoft's System Center Configuration Manager (SCCM) for managing Windows-based computer system. Configuration Manager provides remote control, patch management, software distribution, operating system deployment, network access protection, and hardware and software inventory.

For Unix Solaris related systems, FDIC currently manually downloads the patches and deploys from the soft depot repository. FDIC plans to use Oracle Enterprise Manager Ops Center for management of Solaris operating systems in the future.

In addition, as a part of the Vulnerability Management Process, FDIC identifies the specific servers/desktops with missing patches. Through the eForms process these issues are reported back to an operations point of contact for remediation.

#### 3.4.1.5 Information system component inventory

FDIC uses Remedy as the Asset Repository where software license information is stored in the Software Contract form within the Asset Management Module. FDIC uses SCCM to determine what is installed on the network for MS-Windows OS devices.

FDIC uses BMC Atrium Discovery and Dependency Mapping (ADDM) to:

- Verify that changes have been approved through the Change Control Board (CCB)
- Accurately capture and baseline the configurations of the development, QA, and production environments
- Report exceptions to configuration baselines, standards and procedures
- Discover servers, network components and specific applications for configuration management control.

The information discovered through ADDM is captured in the Configuration Management Database (CMDB)

### 3.4.2 Information Security Risk Management Program

The Corporation, in carrying out its wide range of responsibilities, employs and manages a complex variety of General Support Systems (GSS), which include a mainframe, midrange computers, a wide area network (WAN), local area networks (LANs), and telecommunications systems. In addition, a number of Divisions and Offices have sponsored the development of Major Applications (MA) and other Minor Applications (MN) that store, process, and transmit sensitive data.

The Corporation is responsible for deploying a risk management framework that identifies and evaluates security weaknesses within FDIC's IT assets (including the GSSs, MAs, and MNs) and minimizes risks to those assets by employing solutions that protect the confidentiality, integrity, and availability of the data that these systems process. To satisfy this responsibility, the Corporation has established the corporate-wide Information Security Risk Management Program.

FDIC conducts the following types of activities to support the continuous monitoring program which are detailed in the following sub-sections:

- IT Security Findings Remediation
- Technical Security Assessment
- Computer Security Incidence Response Team
- Annual FISMA self-assessment
- Privacy assessment activities
- Data Loss Prevention
- Malware scanning, detection, remediation
- Host and network-based intrusion detection
- Host security policy compliance assessment

- Continuous Controls Assessment
- Network defense, detection, and monitoring
- SDLC security and privacy surveillance
- IT Project Security and Privacy Consulting

### 3.4.2.1 IT Security Findings Remediation

(b)(5)

[redacted]

### 3.4.2.2 Technical Security Assessments

The FDIC has a robust Technical Security Assessment (TSA) program that provides continuous monitoring of FDIC's application and infrastructure components. These programs are based on a detailed methodology for identifying, assessing and reporting on targeted application and infrastructure components. This program is separate from audits such as those conducted by the FDIC Inspector General (IG) or the Government Accountability Office (GAO).

The FDIC routinely tests GSSs and MAs and their components as part of the CCA activities and in support of the Security Assurance and Authorization (SAA) Program. Activities include tactical assessments of FDIC applications that are useful in uncovering application logic weaknesses in addition to general infrastructure vulnerabilities. The TSA program is designed to identify the most commonly exploited application-level and/or infrastructure-level vulnerabilities and leverages OWASP standards for testing.

The FDIC's implementation of the TSA program is a selective assessment of the relevant applications and infrastructure components. To conduct a TSA, the application inventory is reviewed and prioritized based on: a) risk posed to the organization by the application; b) accessibility of the application; and, c) likelihood of vulnerability exploitation. The TSAs are summarized in reports to management detailing the status of the security posture of the systems under review.

### 3.4.2.3 Computer Security Incident Response Team (CSIRT)

The FDIC Computer Security Incident Response Team (CSIRT) provides a means to detect, report, and respond to computer security incidents within the Corporation's environment. FDIC responds to incidents generated from various sources including:

- Vendor initiated alerts and patches
- Advisories from other security alert teams
- Web-enabled sites for alerts and bulletins
- End user notifications
- US-CERT and law enforcement agencies
- FDIC SOC (Security Operations Center)

- ISPS Personnel

The FDIC has a Security Operation Center (SOC) which focuses its efforts on monitoring of security alerts and researching suspected security events. The SOC monitors alerts from numerous security tools, such as Firewalls, Intrusion Detection/Prevention Systems, and Malware Protection Systems. These alerts are then analyzed in conjunction with research from external parties, as well as collaborative internal information, including: operating system logs, network device logs, network flow data and captured sessions, When sufficient evidence is discovered to determine that an actual security event has occurred the SOC will provide the CSIRT with description of the event at hand as well as a recommended course of action for addressing said security event.

### 3.4.2.4 Annual FISMA self-assessment

As required by FISMA, the FDIC conducts annual information systems assessments of the corporation's GSS and Major Applications, as well as their aggregated minor applications. The self-assessments are based on NIST SP 800-53 controls and cover management, operational and technical controls.

### 3.4.2.5 Privacy assessment activities

Section 208 of the E-Government Act of 2002 requires all Federal government agencies to conduct Privacy Impact Assessments (PIA) for all new or substantially changed technology developed or procured by FDIC that collects, maintains, or disseminates personally identifiable information (PII) or any other electronic collection activity or process that involves PII. A PIA is a documented analysis of how PII is collected, stored, protected, shared and managed. It demonstrates that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. In order to determine if an IT system or electronic collection activity requires a PIA, the first step is to complete a Privacy Threshold Analysis (PTA). The PTA is used to determine and document the need for a PIA or other privacy compliance document (e.g., new or modified Privacy Act System of Records Notice or Privacy Act Statement), and is required for all applications, systems, non-applications, utilities, COTS products, and General Support Systems. The PTA and PIA requirement are also incorporated into the FDIC Outsourced Information Service Provider Methodology.

In addition, privacy staff conducts physical walk-throughs to detect and remediate privacy issues, responds to privacy breaches, performs in-depth assessments of key business processes involving sensitive PII, manages a data loss prevention initiative, and provides consulting services and privacy awareness training to comply with federal and agency-level privacy protection requirements.

### 3.4.2.6 Data Loss Prevention (DLP)

(b)(5) [redacted] DLP is used for detection and prevention of PII and or sensitive information
(b)(5) transmission via unsecured protocols. [redacted] DLP generates automated email alerts and is monitored by ISPS staff.

#### 3.4.2.7 Malware scanning, detection, remediation

(b)(5)

[redacted]

#### 3.4.2.8 Host and network-based intrusion detection

(b)(5)

[redacted]

#### 3.4.2.9 Host security policy compliance assessment

(b)(5)

[redacted]

#### 3.4.2.10 Continuous Controls Assessment

The Continuous Controls Assessment (CCA) Program replaces the "ST&E" process by ensuring risk-based control selection for security compliance testing. The program has evolved from testing all NIST controls on every MA or GSS every three years or upon significant change, to testing controls on a risk and frequency-based determination. To provide information assurance for FDIC's assets, many factors are considered during control selection, such as: criticality of the system, the application, or the component; applicability of controls to system components; relevance of a system update or change to specific NIST controls and to the security posture of the system; and appropriateness of testing frequencies.

The CCA evaluates the effectiveness of the security controls employed in the information system to ensure the confidentiality, integrity, and availability of both the information system and the data it contains. The CCA facilitates the determination of overall risk posture resulting from vulnerabilities in the system. It also serves to support the Security Assurance and Authorization

Program by providing the Authorizing Official (AO) with the security posture of the system. The CCA Report details the results of the assessment activities, where potential impacts of vulnerabilities are tested and evaluated, and provides mitigation recommendations to stakeholders.

In order to evaluate the security posture of the information system on a continuing basis, a determination must be made on what controls need to be monitored and what frequency denotes 'continuous' monitoring. It is necessary to leverage existing automated tools to assist in this effort; specifically, NIST states that "near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF including authorization-related activities".

### 3.4.2.11 Network defense, detection, and monitoring

(b)(5)

### 3.4.2.12 SDLC security and privacy surveillance

ISPS participates as an intersecting organization in the system development process which ensures that we have active security and privacy surveillance activities built into the development lifecycle. ISPS involvement includes security and privacy characterization, risk assessment, creation and check-in of appropriate security and privacy artifacts, and participation in both the change control board (CCB) and the production readiness reviews (PRR) for all infrastructure and application system changes prior to their release into production.

### 3.4.2.13 IT Project Security and Privacy Consulting

ISPS provides security and privacy consulting by creating or vetting security architecture designs, ensuring appropriate security and privacy language is incorporated into contractual agreements, conducting privacy impact assessments of FDIC business processes, reviewing new collections of personally identifiable information, and performing in-depth privacy risk assessments of bank closing processes. ISPS helps create system of record notices for Privacy Act systems when needed, and addresses ad-hoc questions relating to security and privacy guidance including interpretation and implementation of NIST standards for information systems. ISPS also participates on technical evaluation panels for IT related contracts.

### 3.4.3 Security Impact Analysis (SIA)

As part of the information security risk management activities, the FDIC performs security impact assessments (SIA) whenever information systems undergo considerable changes in functionality, software, and or supporting hardware. Significant change determinations are made within the RUP SDLC process. For systems that are going through changes or are impacted by events, the SIA process is used to determine if change is significant and if testing is required.

### 3.4.4 Security Status Monitoring and Reporting

FDIC maintains a cache of tools to monitor and report on the status of security weaknesses and vulnerabilities. [redacted]

(b)(5)

(b)(5)

[redacted]

#### 3.4.4.1 Real-time security monitoring

(b)(5)

[redacted]

#### 3.4.4.2 Periodic security monitoring

(b)(5)

[redacted]

#### 3.4.4.3 eForms

(b)(5)

[redacted]

#### 3.4.4.4 Software Security Assurance

(b)(5)

[redacted]

[9] Refer to the *Vulnerability Management Process Overview* document for details.

### 3.4.4.5 Monthly & quarterly reports

Monthly and quarterly reports from the VM process provide graphs and information about the status of vulnerabilities that exist in the environment along with newly discovered vulnerabilities. These reports are constantly evolving as operations/management's information needs change.

### 3.4.4.6 FDIC's regulatory compliance view

The Corporation uses many tools to monitor agency-wide compliance with federal regulations, statutes, and agency policies.

(b)(2),(b)(5)

[redacted]

### 3.4.4.7 CyberScope reporting

OMB Memorandum 10-15 provides instructions for meeting federal agency reporting requirements under the Federal Information Security Management Act (FISMA) of 2002 which has subsequently been updated in 2014. It also recommends that agencies use CyberScope for annual FISMA reporting. FDIC provides three section reports through CyberScope:

- Chief Information Officer
- Senior Agency Official For Privacy
- Inspector General

### 3.4.5 Active Involvement of Organizational Officials

Based on FISMA requirements, FDIC maintains an Information Security Risk Management Program. In addition, cross-divisional management involvement in our risk management framework includes Directors, Deputy Directors, Managers, System Owners, and Information Security Managers (ISMs). Agency officials and executive groups include:

- Chief Financial Officer (CFO)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Chief Privacy Officer (CPO)
- Chief Risk Officer (CRO)
- CIO Council
- Corporate Management Control (CMC) [formerly OERM]

Organization Officials and Senior Management are actively involved in:

- oversight of information security risk management activities,
- data privacy protection,
- implementation of Corporate-wide policies and procedures,
- responding to regulatory compliance audits,
- assessment and authorization of FDIC's systems and applications,
- Configuration Management (CM) and Change Control Board (CCB) decisions
- FDIC's RUP SDLC
- Network Review Board (NRB)
- Collaborative Working Group (CWG)

## Appendix A: Acronyms

| | |
|---|---|
| ADDM | Atrium Discovery and Dependency Mapping |
| CCA | Continuous Controls Assessment Program |
| CCB | Configuration Control Board |
| CFO | Chief Financial Officer |
| CIO | Chief Information Officer |
| CIS | Center for Internet Security |
| CISO | Chief Information Security Officer |
| CM | Configuration Management |
| CMC | Corporate Management Control |
| CMDB | Configuration Management Database |
| ConMon | Continuous Monitoring |
| CPO | Chief Privacy Officer |
| CRO | Chief Risk Officer |
| CSIRT | Computer Security Incident Response Team |
| CWG | Collaborative Working Group |
| DISA | Defense Information Systems Agency |
| DLP | Data Loss Prevention |
| EA | Enterprise Architecture |
| FISMA | Federal Information Security Management Act |
| GSS | General Support Systems |
| IDS | Intrusion Detection Systems |
| ISB | Infrastructure Support Branch |
| ISM | Information Security Manager |
| ISPS | Information Security and Privacy Staff |
| ISRM | Information Security Risk Management Program |
| JAMES | Joint Audit Management Enterprise System |
| MA | Major Applications |
| MN | Minor Applications |
| NIST | National Institute of Standards and Technologies |
| NOC | Network Operations Center |
| OERM | Office of Enterprise Risk Management (OERM) |
| OIG | Office of Inspector General |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| POA&M | Plan of Action and Milestone |
| PPR | Post Project Review |
| PRR | Production Readiness Review |
| PTA | Privacy Threshold Analysis |
| REF | Risk Executive Function |
| RMF | Risk Management Framework |
| RUP | Rational Unified Process |
| SAA | Security Authorization and Assessment Program |
| SCCM | System Center Configuration Manager |
| SDLC | System Development Life Cycle |
| SIA | Security Impact Analyses |

| | |
|---|---|
| SOC | Security Operations Center |
| SPCS | Security Privacy and Compliance Section |
| SPES | Security Protection Engineering Section |
| ST&E | Security Test & Evaluations |
| TSA | Technical Security Assessment |
| VM | Vulnerability Management |

FEDERAL DEPOSIT
INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Information Security Risk Management (ISRM) Program

# Continuous Controls Assessment (CCA) Methodology

May 2015

This document contains confidential information for FDIC Official Use Only. It shall not be duplicated, used, or disclosed in whole or in part without prior written permission from the Information Security and Privacy Staff.

## Revision History

| Version | Change Comments | Date | Author |
|---|---|---|---|
| 0.1 | Initial Draft | 7/2012 | [redacted] |
| 0.2 | Update | 8/2012 | [redacted] |
| 0.3 | Edits/Update | 8/2012 | [redacted] |
| 1.0 | Update | 8/2012 | [redacted] |
| 1.1 | Update | 9/2013 | [redacted] |
| 1.2 | Update | 10/2013 | [redacted] |
| 1.3 | Update | 11/2013 | [redacted] |
| 2.0 | Update | 3/2015 | [redacted] |
| 2.1 | Update | 5/2015 | [redacted] |

(b)(5),(b)(6)

## Authors

(b)(5),(b)(6) [redacted]
Information Security Assurance
Federal Deposit Insurance Corporation
3501 N. Fairfax Drive
Arlington, VA 22226

(b)(5) [redacted]
3501 N. Fairfax Dr.
Room A-5114
Arlington, VA 22226

# Table of Contents

# Table of Figures

# 1 INTRODUCTION

## 1.1 PURPOSE

The Federal Deposit Insurance Corporation's (FDIC) Continuous Controls Assessment (CCA) Methodology provides an overview of the CCA processes performed for all FDIC owned and/or operated information systems. The CCA process is an integral part of FDIC's overall Information Security Assurance (ISA) Program.

> *"Knowing and fixing problems before cyber adversaries discover them is the fundamental operating objective..."*[1]

## 1.2 BACKGROUND

Continuous monitoring is an integral component in the Risk Management Framework (RMF) outlined in NIST SP 800-37, Revision 1, *Applying the Risk Management Framework to Federal Information Systems* (February 2010). Additionally, OMB M 14-03, *Enhancing the Security of Federal Information and Information Systems,* calls for federal agencies to develop and integrate a continuous controls testing regime for all federal information system.

The objective of FDIC's CCA program is to apply the principles of 800-37 by evolving the former Security Testing and Evaluation (ST&E) Program by using control selection to develop, at the core, a risk-based approach to the security assessment process. In order to do so, the FDIC must proactively determine if the complete set of planned, required, and deployed IT security controls within an information system, or inherited by a system, continue to be effective over time. To meet the new NIST RMF requirements and as part of the overall corporate ISRM Program strategy, the FDIC developed the Continuous Controls Assessment (CCA) program. Characteristics of the CCA Program include:

- Independent and impartial assessments for organizational information system;
- Dynamic and frequent risk-based assessments that focus on specific IT security controls;
- Enhanced communication and collaboration among assessment teams through the use of technologies and processes;
- Use of automation to provide management with near real-time metrics to use when making cost effective and risk-based decisions (including the authorization of information systems);
- Equal emphasis on the selection, implementation, assessment, and monitoring of security controls;
- Integration of information security more closely into the enterprise architecture and system development life cycle (Rational Unified Process (RUP));
- Assignment of responsibility and ownership of controls to staff, as well as establishing control dependencies (control inheritance) amongst systems.

## 1.3 AUDIENCE

This document is intended for all personnel participating in CCA processes and serves as a reference for FDIC's CCA methodology and processes.

[1] Department of Homeland Security, *Information Security Continuous Monitoring Concept of Operations (ISCM CONOPS)*, Version 1.2, February 24,2012

# 2 CONTINUOUS CONTROLS ASSESSMENT METHODOLOGY

## 2.1 Methodology Overview

In support of the FDIC ISA Program, the CCA activities contain a set of robust, recognizable and repeatable process for the assessment and on-going monitoring of information systems that follow the requirements as set forth by NIST and other federal guidance (see Appendix A of this document for a complete list). This federal guidance is recognized as sufficient to secure federal IT resources and has been the *de facto* standard for several years.

All FDIC information systems are required to undergo independent security assessments that are separate and distinct from required, annual Federal Information Security Management Act (FISMA) self-assessments performed by federal staff. The breadth and scope of these independent assessments differ depending on when the assessment occurs within the information system's lifecycle:

- Full Security Assessments (FSA) – Will be conducted prior to the deployment into a production environment of a ***new*** Major Application (MA) and General Support System (GSS). The scope of this assessment includes a comprehensive review of **all applicable** security controls within the information system's authorization boundary. Results from the FSA quantifies the system security posture and contributes to the Authorizing Official's (AO) determination of "acceptable risk" for which an Authorization to Operate (ATO) can be issued.[2]

- Ongoing Security Assessments (OSA) – Are frequent and continuous assessments that focus on **specific, applicable** NIST SP 800-53 security controls in support of the ongoing security authorization process for all FDIC information systems with an ATO. Depending upon system criticality, risk determination, and control selection, relevant controls for FDIC's systems will be assessed at appropriate intervals over a 5-year period. With the on-going nature of the CCA process and constant changes in technology, information systems may be subject to ad-hoc assessments of controls outside of the control assessment frequencies shown in Figure 3 (Section 2). For example, an OSA may be conducted upon a determination of "significant change" to an existing, authorized information system following a security impact analysis. This type of OSA would identify the controls affected by the significant change and assessed accordingly, regardless of the pre-defined assessment frequencies shown in Figure 3.

[2] Detailed information regarding FDIC's Security Authorization Program (SAP) can be found in the FDIC *Security Authorization Program Methodology* document.

### 2.1.1 Assessment Prerequisites

Prior to beginning the assessment process, the following security related artifacts (pertaining to the information system to be assessed) are necessary:

1. System Categorization (from a FIPS 199 analysis)
2. Updated System Security Plan (SSP) – including controls designed to mitigate systematic risks identified during a risk assessment
3. Risk Assessment Report[3]
4. Contingency Plan / Disaster Recovery Plan

Additional information about the security artifacts listed above can be found in Appendix C below.

## 2.2 Assessment Roles and Responsibilities

### 2.2.1 Evaluation Team Composition

The CCA Team consists of security test engineers responsible for test planning and execution, evaluation of results, and development of the information system's Security Assessment Report. The FDIC information system owners and related staff provide the CCA Team with support in the planning, execution, and analysis phases of the assessment process. The specific roles and responsibilities are defined as follows:

**Executives**

- AO: Understands and formally accepts the risk to organizational operations and assets, individuals, other organizations based on the implementation of a defined set of security controls, and the current security state of the information system.[4]
- ISA Program Manager: Serves as the Certifying Official at the FDIC. Implements the CCA program and manages the CCA Team. Communicates with FDIC executives, support staff for the divisions, Information Security Manager (ISMs), and System Owners. Briefs the AO on security posture of systems under evaluation and the residual risk resulting from unmitigated findings documented in the CCA Report results. Provides ATO recommendations to AO.

**CCA Team (Evaluators)**

- Test Lead: Facilitates a smooth operation during the assessment and serves as the primary point of contact for assessment activities. Finalizes the CCA Report.
- Security Test Engineers: Assist in developing plans and procedures, provide test execution guidance, perform an analysis of the results, and prepare the draft and final reports.

[3] Assessments of risk could be any assessment performed that evaluates the risk of a given system or application, including but not limited to: TSAs, FISMA self-assessments, Security Plans, CCA assessment, etc. See Appendix C for more information.

[4] NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, (February 2010)

**System Support Personnel**

- ISM: Provides support to the assessment and serves as the primary point of contact for dissemination of security related information to the system.
- System Owner: Provides support to the assessment.
- Area Specialists: Serve as subject matter experts (SME) and are responsible for subject areas evaluated.

## 2.3 Assessment Approach and Test Methodology Phases

The methodology implemented to conduct an assessment of FDIC owned/operated information systems consists of the following six (6) distinct phases: 1) Initiation, 2) Planning, 3) Preparation, 4) Execution, 5) Results Analysis, and 6) Reporting. These phases are executed using a sequential process flow that begins with the CCA Team performing Initiation, Planning, and Preparation Phase related activities in order to determine the assessment scope. Once determined, the CCA Team begins the Execution Phase by collecting, examining, and testing relevant system artifacts. During the Execution phase, the CCA Team collaborates with system owners, SMEs, ISMs, and other relevant staff to complete the requirements of the assessment. During Results Analysis, the test results are compiled and analyzed to determine the implementation status for the assessed controls. Finally, the assessment results are loaded into the CCA database to support CCA reporting requirements.

Figure 1 (below) provides a graphical representation of the described process flow.

Page 054 of 157

(b)(2),(b)(5)

### 2.3.1 Phase 1: Initiation

#### 2.3.1.1 Initiation Phase Activities

Successful completion of an assessment requires coordination of activities and resources between the CCA Team and the system's management and operational personnel. To facilitate this process, the following items are distributed to key players:

- System Owners and ISMs: Are provided with an information brief, detailing the FDIC assessment process and key procedural elements.
- CCA Team: Requests from the ISM pertinent system documentation for review and testing preparation. This includes artifacts that are completed during a system's security authorization life cycle such as a System Security Plan, Risk Assessment Report or Application Security Assessment (ASA), Memorandum of Agreements (MOAs), Interconnection Security Agreements (ISAs), Plan of Action and Milestones (POA&M), Disaster Recovery Plan, and Configuration Management Plans/Procedures among others.

### 2.3.2 Phase 2: Planning

The Planning phase mobilizes the CCA Team and federal staff to assemble the documentation and artifacts necessary for the CCA Team to understand the system design and components and, ultimately, the assessment project's scope. Following the data gathering, the CCA Team designs a detailed plan for carrying out CCA activities. The CCA Project Plan sets the schedule for all test and evaluation activities going forward and establishes a timetable for testing security control requirements.

#### 2.3.2.1 Control Selection and Applicability

Based on FDIC's requirements to execute, the CCA Team will assess all controls based on the information system's "high water mark" (as a result of the FIPS 199 security categorization process) and as prescribed by the (default) NIST SP 800-53 security control baseline. (Note: At the FDIC, all MAs and GSSs maintain a FIPS 199 categorization of "Moderate".) Control applicability is based on 1) the technologies employed within information system, 2) the information system's logical and physical location, 3) and inherited controls[5].

#### 2.3.2.2 Control Assessment Frequency

To ensure that assessment data is provided in a timely manner to support risk-based security decisions and to provide assurances that the implemented security controls adequately protect organizational assets, the FDIC has assigned assessment frequencies based on the control's 1) impact on FDIC mission critical assets and/or sensitive data, 2) impact on individual systems or across the FDIC enterprise, 3) effectiveness to meet required results (based on trends from previous assessment and audit data), and/or 4) level of acceptable risk within the corporation. The effort to define control criticality is an ongoing process that will evolve as changes occur to risk levels, risk tolerance, and technology. For example, when new attack vectors and patterns arise, the corporation will need to find corrective measures, new strategies and tools, to mitigate new risks. To determine the control assessment frequency, the CCA program used the following risk-based approach, as shown in Figure 2 (below):

[5] The terms 'deferred' and 'inherited' may be used interchangeably (please see *Appendix B – Glossary* for more information).

Page 55

Page 056 of 157

(b)(5)

Page 057 of 157

(b)(5)

The complete set of IT security controls prescribed by NIST for Moderate-baseline systems, which is commensurate with FDIC's FIPS 199 ratings for all GSSs and MAs, are assessed at designated frequencies to ensure that each *applicable* control is examined within a five-year period. Figure 4 (below) illustrates the dynamic nature with which OSA testing is performed and results accumulated to form an information system security baseline that supports an ongoing authorization process during a five-year cycle.

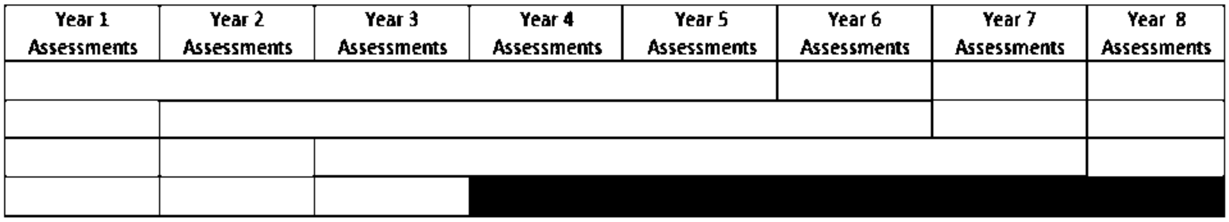


***Figure 4 – Ongoing Authorization Cycles***

For Year 1, previous assessment results for selective information systems were considered and reused as appropriate to start the baseline for the CCA five-year cycle. The CCA Team reviewed and/or analyzed these results to determine the extent to which those results are still applicable and accurately reflect the current security state of the information system.

### 2.3.3 Phase 3: Preparation

In order to prepare for the testing of a system's security controls, the CCA Team must first create a set of documents that describes their approach to the evaluation, the controls that are to be tested, and the requirements that mandate the implementation of those controls. As such, all parties are aware of the nature of the testing to be performed, and changes can be made where appropriate. CCA testing schedules are subject to change due to modifications in organizational priorities, risk levels, changes in scope, and resources limitations.

### 2.3.4 Phase 4: Execution

Execution of the CCA involves a hands-on validation of the proper implementation and function of the IT security controls identified by the CCA Team. The execution process could be comprised of requirements testing, vulnerability scanning, and application testing.

#### *2.3.4.1 Requirements Testing*

The CCA Team conducts testing pertinent to the management, operational, and technical security controls for this system. Interviews, documentation review, direct observation, and direct control testing are the primary methods used to validate compliance with stated requirements. The following control areas are evaluated:

- **Management Controls:**
    - Planning (PL)
    - Program Management (PM)
    - Risk Assessment (RA)
    - Security Assessment and Authorization (CA)
    - System and Services Acquisition (SA)

- **Operational Controls:**
  - Awareness and Training (AT)
  - Configuration Management (CM)
  - Contingency Planning (CP)
  - Incident Response (IR)
  - Maintenance (MA)
  - Media Protection (MP)
  - Physical and Environmental Protection (PE)
  - Personnel Security (PS)
  - System and Information Integrity (SI)

- **Technical Controls:**
  - Access Control (AC)
  - Audit and Accountability (AU)
  - Identification and Authentication (IA)
  - System and Communications Protection (SC)

Compliance with the stated security control requirement is assessed by one or more testing methods, as deemed appropriate. This determination of control implementation compliance is based upon the efficacy of supporting evidence. For aggregated minor applications that meet one or more identified risk conditions (refer to Section 2.4.2), distinct testing is performed to ensure that the confidentiality, integrity, and availability of the data are maintained. To ensure due diligence while avoiding undue expense, specific applicable controls from four control families are assessed for applicable minor applications that include:

- Identification and Authentication (IA)
- Access Control (AC)
- Audit and Accountability (AU)
- System and Communications Protection (SC)

Furthermore, assessment of other security controls may be included as deemed necessary for minor applications.

#### *2.3.4.2 Application Testing*

The independent assessment team also specializes in identifying the most commonly exploited application-level vulnerabilities that exist within FDIC's infrastructure. The methodology used is heavily influenced and guided by Open Web Application Security Project (OWASP) best practices. The OWASP project maintains a current listing of the most common application vulnerabilities. Based on: a) risk posed to the organization by the system, b) accessibility of the system and, c) likelihood of vulnerability exploitation, the assessment team may perform additional testing to determine if exploitable application-level vulnerabilities exist and provide remediation recommendations.

#### *2.3.4.3 Vulnerability Scanning*

The assessment team performs vulnerability scanning (technical testing) on an information system in order to identify IT assets that are susceptible to known vulnerabilities. The tools and technologies used to perform the technical scans that may include the following open-source and commercial off- the-shelf (COTS) products:

(b)(5)

[redacted]

The information gleaned from vulnerability scans is tracked by the Infrastructure Assessment Team. After performing the vulnerability scan, it is necessary to implement a process for mitigating identified vulnerabilities. Typically, there are patches or updates available that address these problems. In some cases, there may be operational or business reasons where applying the patch is not advised and other alternatives to mitigate the threat must be developed.

### 2.3.5 Phase 5: Results Analysis

Subsequent to the completion of an assessment, the test case results are reviewed and scrutinized, findings are identified and documented, potential impact of failed controls is determined, and recommendations for mitigation are developed. Any discrepancies in test results are mitigated by either re-testing the control or acquiring additional information related to its implementation from federal staff.

### 2.3.6 Phase 6: Reporting

Any security control found to be deficient during the testing and evaluation process is documented in the CCA Report. The compiled results are reviewed and approved by the CCA Program Manager. Once approved, the CCA Program Manager issues the final CCA Report to Division Directors, Division Management, ISMs, System Owners, ISPS staff, as appropriate.[6] Based on the findings, the System Owner, Program Manager, and ISMs employ a POA&M to manage the mitigation and closure of findings. The System Owner and ISM can begin to coordinate activities such as:

- Mitigation of identified vulnerabilities within the system environment and modification of the POA&M, as required.
- Updating the Risk Assessment and/or System Security Plan to reflect findings of the assessment.
- Providing required and/or optional artifacts to support the security authorization process.
- Planning for future security activities.

In accordance with FISMA and FDIC regulations, the POA&M must be kept up-to-date with ongoing enhancements and deficiency remediation throughout the lifecycle of the system. This action enables management to remain abreast of the potential risks posed by the continual operation of the system and any new risks that may have been introduced to the environment as a result of changes to the baseline configuration.

[6] The Authorization Official is a representative among the Division Directors group. Detailed information regarding FDIC's Security Authorization Program (SAP) can be found in the FDIC *Security Authorization Program Methodology* document.

The FDIC employs an open source POA&M management tool called OpenFISMA. Findings identified during the assessment are uploaded into OpenFISMA for real-time tracking of remediation activities within the security life cycle, specifically during the risk mitigation, corrective action validation, and closure processes. Following completion of remediation activities for specific assessment findings against an application, system, or its supporting infrastructure, control failures are re-tested by the CCA Team to ensure the corrective actions have properly mitigated the control failure. When the previously deficient control is verified as in place and performing as required, the finding is closed within OpenFISMA.

The CCA Report and the POA&M identify the security posture of the information system under review and provide the ISA Program Manager, serving as the FDIC's Certifying Official, with the requisite information needed to evaluate the system's residual risk and make an authorization recommendation to the AO. The CCA Program uses the reporting capabilities within OpenFISMA, which includes several management dashboards that can summarize or detail the CCA compliance results for all of FDIC's GSSs, MAs, and Minor Applications (MNs).

### 2.3.7 Leveraging Previous Assessment Results

Since the costs associated with independent security assessments can be substantial, it is important to leverage the results of previous assessments and audits conducted on an agency's information system or on the components that comprise that system. Several potential sources of previous assessment data for consideration include: (i) commercial product testing and evaluation programs; (ii) privacy impact assessments; (iii) physical security assessments; (iv) self-assessments; (v) ad hoc technical security assessments; and (vi) internal and external audits. Data obtained from these sources can support the security authorization processes in two important ways. First, the assessment and audit results can be used to gauge the preparedness of an information system for security authorization by examining the status of key security controls in the system. Second, the results produced during these assessments and audits can be considered and potentially reused, when appropriate, during the security authorization process. Previous assessment and audit results should always be reviewed and/or analyzed to determine the extent to which those results are still applicable and accurately reflect the current security state of the information system. Where previous results are deemed not fully applicable or not current, those areas should be reassessed or the differences properly noted. Collecting assessment and audit results from multiple sources, both internal and external, provides additional assurances that the security controls in an information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This not only reduces the potential cost of the security authorization process, but also increases the overall confidence in the final results. Reuse and sharing of security control assessment-related information can result in a more consistent application of agency-wide security solutions. To support this process, the CCA Team developed and currently maintains a centralized database repository for the collection and distribution of CCA data. Reports generated from the database can provide management with the near real-time metrics concerning the security posture of FDIC's assets and infrastructure components individually or corporate-wide.

## 2.4 CCA Assessment Implementation Strategies

FISMA allows agencies to design cost-effective information security controls based on the level of risk that is acceptable to the organization. It allows agencies to "identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of (a) information…or (b) information systems." Therefore, agencies can make cost-effective decisions by applying an appropriate level of controls to a system commensurate with its level of risk categorization.

Based on this premise, the CCA process can be adjusted or scoped to meet the security requirements of the information system under assessment. The controls selected are tailored to match the importance of, and risk to the information system, minimizing the asset requirements (costs, staff time) for the conduct of assessments. The FDIC devised an effective control selection process to meet these factors and devised three distinct CCA assessment strategies for the following:

- FDIC Owned/Operated GSSs and MAs
- FDIC Owned/Operated MNs
- Vendor Owned (Outsourced) Information Systems

### 2.4.1 Assessment Strategy for FDIC Owned/Operated GSS and MA

The CCA strategy, either for FSA or OSA, is used when assessing GSSs and MAs that are owned and operated by the FDIC.

#### *2.4.1.1 Common Security Controls and Deferred Authority Assessment Strategy*

NIST SP 800-53 provides a comprehensive suite of security controls commensurate with the totality of protection a system requires to operate within the federal space; however, it is frequently found that several information systems within an organization can capitalize on the same security infrastructure and share common protection mechanisms amongst multiple systems. NIST SP 800-37 outlines the concept of "Common Security Controls," or those controls that can be considered shared resources within an organization. Because the management of these processes and procedures is typically outside the scope of any one system, each organization must develop a methodology for addressing the weaknesses identified in these control categories.

Within the FDIC infrastructure, ISPS has identified 86 individual security controls (not including enhancements) that can be considered Agency Common Controls (ACC). Agency Common Controls are assessed independently of the GSS or MAs. Common controls fall outside the immediate management authority of the information System Owner. However, System Owners and ISMs remain responsible for ensuring proper implementation of common controls on their systems.

Additionally, because of the unique differentiation between the hardware and software environments at the FDIC, there are some instances where a system may rely on its supporting infrastructure to provide security protections above and beyond those discussed in the common controls area. When that is the case, the SSP must depict the control as "Met" and document the deferral to the external component to which the system is relying upon in the Security Control Implementation Details section. In this manner, the System Owner is able to differentiate between those weaknesses that are his/her immediate responsibility, and those that will require coordination with external entities in order to mitigate.

### 2.4.2 Assessment Strategy for FDIC Owned/Operated Minor Applications

At FDIC, all minor applications are aggregated under a parent GSS or MA in order to ensure proper evaluation of security control implementation consistent with the size, scope, and risk exposure of the minor application. The *Systems Aggregation Methodology*, dated April 17, 2007, details the process employed by the FDIC to aggregate minor applications under parent MAs or GSSs. Due to the large number of minor applications, FDIC has identified criteria to determine which of these specific assets will be assessed against NIST SP 800-53 controls. Due to the nature of a "minor" application (generally "lower-risk" than a MA or GSS), FDIC has focused on applying an appropriate level of security scrutiny and proper expenditure of resources on testing through control selection. To determine the necessity of assessing a specific minor application against applicable NIST controls, a minor application must meet one or more of these conditions:

- Condition 1: The application is identified as mission critical
- Condition 2: The application is publicly accessible via the internet
- Condition 3: The application stores or processes sensitive personally identifiable information (PII)
- Condition 4: The application is identified as financial system

Minor applications that meet either Condition 2, 3 or 4 will undergo a limited technical security assessment only. However, if Condition 1 or more than one condition (from Condition 2 through 4) is met, the application will be tested using the previously established NIST technical security controls referenced in Section 2.3.4.1.

If any of the above conditions are identified for a minor application within FDIC's system inventory repository, EA-REP, testing will be conducted on a three-year cycle to ensure that the confidentiality, integrity, and availability of the data within the minor application are maintained. The extent of testing is at the discretion of the assessment team.

### 2.4.3 Assessment Strategy for Vendor Owned (Outsourced) Information Systems

For outsourced information systems, the FDIC will follow the guidance within the *FDIC Outsourced Vendor Assessment Methodology*, which is presently outside the scope of this CCA Methodology.

# APPENDIX A – GUIDANCE

- Title III of the E-Government Act of 2002, Federal Information Security Management Act (FISMA)
- OMB Circular A-130, *Management of Federal Information Resources*
- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*
- NIST Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
- NIST SP 800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems*
- NIST SP 800-53A Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

# APPENDIX B – GLOSSARY

This section provides definitions for security terminology used within the Continuous Controls Assessment Methodology. Unless otherwise specified, all terms used in this publication are consistent with the definitions contained in Committee on National Security Systems (CNSS) Instruction 4009, National Information Assurance Glossary.

Authorization (to operate)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorization Boundary

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorize Processing

See *Authorization*.

Authorizing Official

A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Common Control

A security control that is inherited by one or more organizational information systems.

See *Security Control Inheritance*.

Deferred Control

See *Security Control Inheritance.*

Hybrid Security Control

A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

See *Common Control* and *System-Specific Security Control*.

Inherited Control

See *Security Control Inheritance.*

Ongoing Security Authorization

A subset of RMF. It consists of three recursive steps – assess, re-authorize, and monitor – that are executed to maintain the established security posture baseline. The ISCM technology enables agency security operating personnel to rapidly execute the ongoing security authorization thus maintaining the established security posture baseline.

Security Control Inheritance

A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

See *Common Control.*

System-Specific Security Control

A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Tailored Security Control Baseline

A set of security controls resulting from the application of tailoring guidance to the security control baseline.

See *Tailoring.*

Tailoring

The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

# APPENDIX C – SECURITY ARTIFACTS

### System Categorization (from a FIPS 199 Analysis)

All FDIC application systems shall undergo a process to determine the appropriate FIPS 199 security categorization by examining factors such as the level of the information processed, which indicates the potential impact on FDIC's mission if the confidentiality, integrity, and/or availability of the information systems or its data were compromised.

General Support Systems (GSSs), by their nature, receive a rating equivalent to the highest FIPS 199 rating of the applications they support; at the FDIC, the highest possible application system rating is currently "Moderate". Consequently, a system security categorization is not performed on GSSs; however, all other relevant activities within the Information Security Risk Management Program (ISRM) must be completed for a GSS.

### System Security Plan (SSP)

The introduction of changes to several NIST publications has provided agencies with guidance on minimum standards of IT security controls for federal systems.

The specifics described in NIST SP 800-53 and NIST SP 800-53A provide baseline sets of controls from which agencies can select, as a whole or in part, as applicable. The Corporation applies the NIST "moderate" controls as the baseline set of controls for assessing risk to information systems and may deselect non-applicable controls from that set, when appropriate.

The output from the security control selection process is the System Security Plan (SSP), which documents applicable controls as defined by the FDIC. The purpose of the SSP is to provide a system architecture overview and identify and document the planned and in-place controls; the plan may also identify non-applicable NIST controls for the information system. The SSP is assessed and updated during a period of review of the security controls to ensure the plan accurately depicts what is implemented in the information system.

In addition to the activities of control selection for each system, the Corporation has defined a separate set of Agency Common Controls (ACC) that is inherited by information systems.

### Assessments of Risk

The Chief Information Officer Organization (CIOO) manages and oversees risk assessment activities at Tier 3 (information system level) that include:

1. **Creation of, review of, and/or update to a System Security Plan** – As described above, the SSP encompasses the security controls in place for an information system. An SSP may be reviewed and updated when an information system undergoes a CCA, TSA, significant change to its security posture from an update, or during the annual FISMA self-assessment. When the SSP is reviewed for updates, all security controls are reassessed to ensure they still capture the current state of the information system's security posture.

2. **Creation of, review of, and/or update to Contingency/Disaster Recovery Plans** – Contingency/Disaster Recovery Plans are developed and tested to address measures to be taken in response to a disruption in availability due to an unplanned outage. Contingency Plans describe the recovery of an information system

due to a temporary disruption to, or loss of, that information system. Disaster Recovery Plans describe the process for re-establishing functionality of GSSs after an unplanned service interruption.

3. **Conduct, or create and submit, a Security Impact Assessment (SIA)** – Information systems are typically in a constant state of change, so it is important to understand the impact of changes to their functionality and their existing security controls, and in the context of organizational risk tolerance. Generally, the SIA is incorporated into the documented change management (CM) process. Under circumstances where significant impact to the security posture of an information system is not readily apparent, an SIA may be conducted by the CIOO. In these circumstances, the Security Policy and Compliance Section (SPCS) will determine whether a formal (documented) or informal (discussion) SIA process is to be conducted.

4. **Execution of Continuous Controls Assessment (CCA) Activities:**

   a. ***NIST-related Security Controls Assessments*** – FDIC's information systems are independently evaluated for compliance with management, operational and technical security control requirements as defined in the System Security Plan. Ongoing testing of FDIC's information systems and applications is performed to determine the effectiveness of security controls implementation and may identify weaknesses or control failures that are documented for remediation tracking within a POA&M.

   b. ***Technical Security Assessments (TSA)*** – FDIC's information systems are independently evaluated for compliance with technical security control implementation as defined in the System Security Plan. TSAs also leverage guidance provided by the Open Web Application Security Project (OWASP) and other industry sources for application security, and validate technical controls against FDIC policy.

   c. ***Security Protection and Engineering Section (SPES) Testing*** – Employs automated tools to execute ongoing network scanning and monitoring for configuration baselines, perimeter protection, and vulnerability assessments, with management reporting capabilities. SPES also conducts malware and forensic analysis, incident response, and data loss prevention (DLP).

5. **Security Findings Remediation (POA&M processing)** – A POA&M documents the plan for mitigation activities, or resolution of risks identified during independent CCA activities. All findings and results of NIST-related security control assessment activities, Technical Security Assessments, and SPES testing are reported to the respective FDIC section, branch, or divisional information system owner that requested the assessment or for which the assessment was required. All findings are mapped to specific NIST-related SP controls and entered and tracked in FDIC's POA&M tracking and management tool for eradication or remediation of findings. The tool provides reporting capabilities for management to obtain both corporate-level and system-level risk metrics for determining the security posture of FDIC's information systems. The responsibility for remediating or eradicating findings falls on the respective FDIC information system owner.

6. **Initial Authorization to Operate (ATO) and Continuous Authorization** – An ATO is required well in advance of the complete development and deployment of a new Major Application system into the FDIC production environment, or the production deployment of an existing major information system that undergoes significant change to its security posture. An ATO is also required for all GSSs. Prior to implementation into a production environment, such information systems will be assessed through an independent CCA. Approval of a production deployment and execution of a formal ATO involves senior management officials; generally, an executive from the client Division sponsoring the application (Director) requests the ATO, while the Chief Information Officer (CIO), or his delegate, makes the formal ATO decision. In the absence of any significant

change events to information systems, including GSSs, Continuous Authorization occurs as a function of ongoing CCA activities.

**Contingency Plan / Disaster Recovery Plan**

Contingency and Disaster Recovery Plans are developed and tested to address measures that must be taken in response to a disruption in availability due to an unplanned outage.

- Contingency Plans describe the recovery of an information system due to a temporary disruption to, or loss of that information system.

  Disaster Recovery Plans describe the process for re-establishing functionality of GSSs after an unplanned service interruption.

# FDIC PROGRESS REPORT ON ELIMINATING UNNECESSARY USE OF SOCIAL SECURITY NUMBERS (SSNs)

The Federal Deposit Insurance Corporation (FDIC) collects and uses SSNs where required in the course of conducting its mission, such as in the administration of employee payroll, benefits, travel, and employee on-boarding programs such as issuance of agency badges and conducting background investigations. Additionally, the FDIC collects a significant amount of bank customer information containing SSNs while conducting routine bank examinations and managing receiverships.

A breach of security resulting in the loss or theft of SSNs could result in harm to an employee or bank customer. The FDIC is committed to providing adequate security and business process safeguards over SSNs in order to foster an environment where both employees and the public feel confident that there is a business need for any personally identifiable information (PII) that is collected and maintained by the FDIC, and that such data is adequately controlled and protected.

Under federal laws and regulations, it is the responsibility of the FDIC and each employee and contractor to protect sensitive information against unauthorized use, access, disclosure, sharing, or disposal. In support of these mandates, the FDIC has established the following directives to provide guidance for the appropriate collection, maintenance, use, and/or dissemination of records, especially with regard to SSNs:

- FDIC Circular 1031.1, *Administration of the Privacy Act*
- FDIC Circular 1210.1, *FDIC Records and Information Management (RIM) Policy Manual*
- [redacted]

(b)(5)

- FDIC Circular 1360.8, *Information Security Categorization*
- FDIC Circular 1360.9, *Protecting Sensitive Information*
- FDIC Circular 1360.12, *Reporting Computer Security Incidents*
- FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*
- FDIC Circular 1360.19, *Privacy Impact Assessment Requirements*
- FDIC Circular 1360.20, *Federal Deposit Insurance Corporation (FDIC) Privacy Program*
- [redacted]
- FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*

(b)(2),(b)(5)

- FDIC Circular 2410.6, *Standards of Ethical Conduct for Employees of the Federal Deposit Insurance Corporation (FDIC)*
- FDIC Circular 3700.16, *FDIC Acquisition Policy Manual (APM)*

Privacy Staff also developed a dedicated booklet entitled: *Protecting Sensitive Information in Your Work Area: A Guide for the FDIC*, which is included in orientation packages and handed out to all new hires as an aid to assess, reduce, secure, and safely dispose of sensitive information.

FDIC administers an ongoing agency-wide program, while adhering to the Federal Information Privacy Standards, to highlight the need to protect SSNs/PII and to assess the use of SSNs/PII throughout its business lines and administrative functions. This activity includes evaluating practical alternatives to the use of SSNs, such as having them eliminated; restricted; replaced with a unique employee identification number; or concealed in agency business processes, systems, and electronic forms.

Initiatives in support of FDIC's efforts to eliminate or reduce unnecessary use of SSNs that were completed during the 2015 reporting cycle include the following:

- Implemented an agency-wide awareness campaign entitled: *Privacy – No Appetite for Risk*, aimed at increasing employee and contractor awareness of the need to protect sensitive information including Social Security Numbers (SSNs). The campaign included a global message sent to all employees and contractors, lobby posters displayed throughout all FDIC offices nationwide, earnings and leave statement messages, and TV monitor messages.

- Privacy program, along with security and legal staff conducted nationwide training via the *Privacy and Data Protection Roadshow Regional Tours*. The roadshows were conducted in the New York, Boston, San Francisco, Atlanta, Kansas City, and Chicago regional offices and centered on the following four key privacy and data protection issues impacting FDIC employees' and contractors' work and home lives:

    - Privacy Act 101: How to Avoid Privacy and Legal Pitfalls
    - Staying out of the Headlines: The Top Ten Things You Can Do to Prevent an FDIC Data Breach
    - Cybersecurity for Managers and Employees: Reducing the Agency's Appetite for Risk
    - Starting Privacy Early: Lowering Your Online Profile Risk

- Maintained and updated the internal FDIC Privacy Program website to ensure that FDIC personnel have easy access to an array of privacy resources, policies, procedures, and best practice tips that can be used to better understand, assess, mitigate, and remediate risks to the protection of SSNs held by the agency. The website includes an automated "PII/Sensitive PII Identification Tool" to assist FDIC employees and contractors in their day-to-day work and a reminder about the need to collect and retain sensitive PII/SSNs only when necessary for a FDIC business need.

- Held FDIC's annual agency-wide *Privacy Clean-Up Day* in the agency's continued effort to further assess, reduce, secure, and dispose of unnecessary holdings of SSNs and other PII.

- Performed monthly monitoring and provided enhanced reporting to management of sensitive and non-sensitive materials being shipped via express mail to address the safety and security of PII-related materials during shipment.

- Continued to maintain the use of a web content and compliance monitoring tool to conduct scans of FDIC's Internet website (FDIC.gov) in order to identify and address issues related to the protection of SSNs/PII.

- Performed privacy threshold analyses and privacy impact assessments to track and review new and existing FDIC programs, systems, and applications in order to identify uses of PII and opportunities to reduce and secure SSNs/PII.

- As part of FDIC's Outsourced Information Service Provider Assessment Methodology, continued to conduct security and privacy reviews of contractors responsible for processing significant amounts of sensitive data containing SSNs/PII in order to ensure that appropriate security and privacy clauses were included within the contracts and privacy impact assessments were performed.

- Conducted unannounced privacy walk-throughs at five FDIC regional buildings located in New York, San Francisco, Atlanta, Kansas City, and Chicago to increase employee and management awareness of instances where sensitive data, including SSNs/PII, involving paper or electronic records, could be eliminated, reduced, or better secured.

- Increased the use of an automated data loss prevention tool to monitor and block the sending of unsecured emails containing SSNs/PII outside the FDIC network and notified personnel of the need to use an FDIC-approved encryption method to prevent future policy violations. Also, continued use of the tool to monitor and report on unstructured data located on FDIC's network to ensure that SSNs/PII is identified and appropriately controlled.

- Continued the use of a threat awareness and education program implemented to reduce instances of unintended disclosure/exfiltration of PII and SSNs in social engineering attempts. This awareness training included internal phishing exercises with built-in on-the-spot guidance. If an individual clicks on a phishing email, they are immediately directed to an awareness page with guidance on how to detect future suspicious emails.

- Encouraged the secure transmittal and disposal of material containing SSNs during pre-exit clearances of exiting employees.

In summary, the elimination of unnecessary holdings of SSNs from FDIC's many business processes continues to be a priority, as are the overall efforts to ensure the integrity, security, and safe handling of all PII to which the agency has been entrusted. While the challenge continues to remain a significant concern, the FDIC is committed to evaluating usage of SSNs throughout the agency and, wherever possible, eliminating the unnecessary collection and use of SSNs.

## FDIC PROGRESS REPORT ON THE REVIEW AND REDUCTION OF HOLDINGS OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

The Federal Deposit Insurance Corporation (FDIC) collects and uses PII where necessary and appropriate to administer payroll, benefits, and employee programs. Additionally, as part of its mission, the FDIC collects a significant amount of bank customer information containing PII in the course of conducting routine bank examinations and managing receiverships.

A breach of security resulting in the loss or theft of PII could result in harm to an employee or bank customer. The FDIC is committed to providing adequate security and business process safeguards over PII in order to foster an environment where both employees and the public feel confident that there is a business need for any PII that is collected and maintained by the FDIC, and that such data is adequately controlled and protected.

Under federal laws and regulations, it is the responsibility of the FDIC and each employee and contractor to protect sensitive information from unauthorized use, access, disclosure, sharing, or disposal. In support of these mandates, the FDIC has established the following directives to provide guidance for the appropriate collection, maintenance, use, and/or dissemination of records:

- FDIC Circular 1031.1, *Administration of the Privacy Act*
- FDIC Circular 1210.1, *FDIC Records and Information Management (RIM) Policy Manual*

(b)(5) [redacted]

- FDIC Circular 1360.8, *Information Security Categorization*
- FDIC Circular 1360.9, *Protecting Sensitive Information*
- FDIC Circular 1360.12, *Reporting Computer Security Incidents*
- FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*
- FDIC Circular 1360.19, *Privacy Impact Assessment Requirements*
- FDIC Circular 1360.20, *Federal Deposit Insurance Corporation (FDIC) Privacy Program*

(b)(5) [redacted]

- FDIC Circular 2150.1, *Pre-Exit Clearance Procedures for FDIC Employees*
- FDIC Circular 2410.6, *Standards of Ethical Conduct for Employees of the Federal Deposit Insurance Corporation (FDIC)*
- FDIC Circular 3700.16, *FDIC Acquisition Policy Manual (APM)*

Privacy Staff also developed a dedicated booklet entitled: *Protecting Sensitive Information in Your Work Area: A Guide for the FDIC,* which is included in orientation packages and handed out to all new hires as an aid to assess, reduce, secure, and safely dispose of sensitive information.

FDIC administers an ongoing agency-wide program, while adhering to the Federal Information Privacy Standards, to highlight the need to protect PII and to assess the use of PII throughout its business lines and administrative functions. During the 2015 reporting cycle, the FDIC's Privacy Program staff performed the following agency-wide initiatives to increase the identification, reduction, protection, and control of PII:

- ➢ Implemented an agency-wide awareness campaign entitled: *Privacy – No Appetite for Risk,* aimed at increasing employee and contractor awareness of the need to protect sensitive information and Social Security Numbers (SSNs)/PII. The campaign included a global message sent to all employees and contractors, lobby posters displayed throughout all FDIC offices nationwide, earnings and leave statement messages, and TV monitor messages.

- Privacy program, along with security and legal staff conducted nationwide training via the *Privacy and Data Protection Roadshow Regional Tours.* The roadshows were conducted in the New York, Boston, San Francisco, Atlanta, Kansas City, and Chicago regional offices and centered on the following four key privacy and data protection issues impacting FDIC employees' and contractors' work and home lives:

  - Privacy Act 101: How to Avoid Privacy and Legal Pitfalls
  - Staying out of the Headlines: The Top Ten Things You Can Do to Prevent an FDIC Data Breach
  - Cybersecurity for Managers and Employees: Reducing the Agency's Appetite for Risk
  - Starting Privacy Early: Lowering Your Online Profile Risk

- Held FDIC's annual agency-wide *Privacy Clean-Up Day* in the agency's continued effort to further assess, reduce, secure, and dispose of unnecessary holdings of SSNs and other PII.

- Maintained and updated the internal FDIC Privacy Program website to ensure that FDIC personnel have easy access to an array of privacy resources, policies, procedures, and best practice tips that can be used to better understand, assess, mitigate, and remediate risks to the protection of PII held by the agency. The website includes an automated "PII/Sensitive PII identification tool" to assist FDIC employees and contractors in their day-to-day work and a reminder about the need to collect and retain PII only when necessary for a FDIC business need.

- Performed monthly monitoring and provided enhanced reporting to management of sensitive and non-sensitive materials being shipped via express mail to address the safety and security of PII-related materials during shipment.

- Increased the use of an automated data loss prevention tool to monitor and block the sending of unsecured emails containing sensitive PII outside the FDIC network and notified personnel of the need to use an FDIC-approved encryption method to prevent future policy violations. Also, continued use of the tool to monitor and report on unstructured data that is located on FDIC's network to ensure that the data is identified and appropriately controlled.

- Continued the use of a threat awareness and education program implemented to reduce instances of unintended disclosure/exfiltration of PII and SSNs in social engineering attempts. This awareness training included internal phishing exercises with built-in on-the-spot guidance. If an individual clicks on a phishing email, they are immediately directed to an awareness page with guidance on how to detect future suspicious emails.

- Continued to maintain the use of a web content and compliance monitoring tool to conduct scans of FDIC's Internet website (FDIC.gov) in order to identify and address issues related to the protection of PII.

- Performed privacy threshold analyses and privacy impact assessments to track and review new and existing FDIC programs, systems and applications in order to identify uses of PII and opportunities to reduce and secure SSNs/PII.

- As part of FDIC's Outsourced Information Service Provider Assessment Methodology, continued to conduct security and privacy reviews of contractors responsible for processing significant amounts of sensitive data containing SSNs/PII in order to ensure that appropriate security and privacy clauses were included within the contracts and that privacy impact assessments were performed.

- Conducted unannounced privacy walk-throughs at five FDIC regional buildings located in New York, San Francisco, Atlanta, Kansas City, and Chicago to increase employee and management awareness of instances where sensitive data, including SSNs/PII, involving paper or electronic records, could be eliminated, reduced, or better secured.

- Encouraged the secure transmittal and disposal of material containing PII during pre-exit clearances of exiting employees.

In summary, the reduction of unnecessary holdings of PII from FDIC's many business processes continues to be a priority, as are the overall efforts to ensure the integrity, security, and safe handling of all PII to which the agency has been entrusted. While the challenge continues to remain a significant concern, the FDIC is committed to evaluating usage of PII throughout the agency and, wherever possible, eliminating the unnecessary collection and use of PII.

FDIC FEDERAL DEPOSIT
INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

# Data Breach Handling Guide

Version 1.4
April 16, 2015

**This document contains confidential information for FDIC Official Use Only**

# TABLE OF CONTENTS

# 1 INTRODUCTION

## 1.1 Background

In the course of meeting its mission to maintain stability and public confidence in the nation's financial system, the Federal Deposit Insurance Corporation (FDIC) collects and maintains a wide range of sensitive information (SI), which includes both **personally identifiable information (PII)** and **agency and business sensitive information (BSI)** that is confidential, proprietary or otherwise restricted in nature. Under Federal law and regulation, the FDIC is responsible for safeguarding such data from loss, theft or compromise ("breach"). Failure to protect sensitive information from a breach could cause significant financial, reputational, operational, or other harm to the Corporation and affected individuals and entities. (Refer to **Section 2** for a complete definition of SI.)

In the event of a data breach, the FDIC recognizes that an effective and quick response is critical to its efforts to prevent or minimize any consequent harm caused by the incident. Depending on the type of breach, an effective response may necessitate notifying affected individuals and entities, as well as sharing information with authorized parties in a position to cooperate, either by assisting in notification to affected individuals/entities or playing a role in preventing or minimizing harms from the breach. The FDIC also recognizes the requirement to report potential losses, no matter how limited the initial information, to comply with Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) guidance.

## 1.2 Purpose

The following *FDIC Data Breach Handling Guide* provides a roadmap for how FDIC addresses data breaches and incidents involving FDIC sensitive information, including BSI and PII. It includes the organizational framework, key definitions, roles and responsibilities, appropriate training, and step-by-step procedures for implementing each stage of the FDIC's incident handling lifecycle including: incident prevention/preparation; detection/discovery; reporting; data collection, investigation, and escalation; analysis and mitigation; external breach notification; closure; and after action review/lessons learned. Additionally, this guide explains the rules and consequences for incidental, accidental and intentional disclosures of BSI and PII. The overarching objective of this guide is to ensure that FDIC responds in a timely and appropriate manner to known or suspected data breaches, not only to protect FDIC information and assets, but also to limit harm to individuals and entities who might be affected by the incident.

This guide supersedes FDIC's *Procedures for Responding to a Breach of Personally Identifiable Information* and *Procedures for Responding to a Breach of Sensitive Information.*

## 1.3 Scope

The provisions outlined in this guide apply to all FDIC employees, contractors, vendors, outsourced providers, and other parties who collect, transmit, process, use, maintain/store, or dispose of FDIC sensitive information in support of the FDIC's mission or for other authorized purposes[1]. This includes data maintained in electronic format (e.g., email, shared drives, websites, systems, etc.), as well as information available in hardcopy (paper) format.

In addition to physical security incidents (e.g., lost/stolen equipment or documents), computer security incidents[2] involving a loss or compromise of sensitive information will trigger the

[1] For example, the U.S. Government Accountability Office (GAO) and other non-FDIC entities may have access to FDIC sensitive information for authorized purposes and should report the loss of such data to FDIC in accord with these procedures.

[2] A computer security incident is an event that threatens the security of the FDIC's "Automated Information Systems (AISs)," including FDIC's computers, mainframe, networks, software and associated equipment.

procedures in this guide. If an incident threatens the security of FDIC's network or systems, FDIC personnel must refer to and follow the FDIC Security Protection Engineering Section (SPES) policies and procedures[3] for computer security incident containment and response. This guide supplements, but is not intended to replace, said SPES policies and procedures.

## 1.4 Legal Authorities and References

These procedures were established in accord with Federal requirements for data breach reporting and response. The primary legal authorities and references for this guidance include:

- **The Privacy Act of 1974** which requires Federal agencies, to among other things, protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

- **The Federal Information Security Management Act of 2002 (FISMA)** which requires Federal agencies to, among other things, establish procedures for detecting, reporting and responding to security incidents, consistent with federal standards and guidelines. Federal agencies are also required to notify and consult with law enforcement agencies and other appropriate entities, including but not limited to reporting incidents to the United States Computer Emergency Readiness Team (US-CERT) office within the Department of Homeland Security (DHS), consistent with the agency's incident response policy.

- **Office of Management and Budget (OMB) memoranda**, including: M-06-15, *Safeguarding Personally Identifiable Information* (May 22, 2006) which reminds agencies of their responsibility to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy. Additionally, M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006); M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* (July 12, 2006); M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007); and (3) *Recommendations for Identity Theft Related Data Breach Notification* (September 20, 2006). Collectively, these OMB memoranda define the appropriate reporting, handling and notification procedures for privacy incidents. OMB also requires agencies to report all privacy incidents to US-CERT within one hour of discovering the incident, and mandates that agency personnel report privacy incidents as soon as possible.

- **Presidential Executive Orders and Task Forces,** including Executive Order 13402, *Strengthening Federal Efforts to Protect Against Identity Theft* (May 2006) which established the Identity Theft Task Force which was charged with making recommendations and developing a strategic plan to strengthen Federal agencies' efforts to protect against identity theft. The task force issued guidance, including but not limited to: the President's Identity Theft Task Force, *Summary of Interim Recommendations: Improving Government Handling of Sensitive Personal Data* (September 19, 2006), which provided guidance to Federal agencies on responding to data breaches, including considerations for determining whether to notify affected individuals; and the President's Identity Theft Task Force Report, *Combating Identity Theft: A Strategic Plan* (updated September 2008), which included a strategic plan for combating identity theft and provided recommendations for establishing a national breach notification requirement and developing data breach response guidance.

[3] Policies and procedures for reporting computer security incidents are outlined in the FDIC Circular 1360.12, *Reporting Computer Security Incidents*. In addition, FDIC Circular 1360.1, *FDIC Automated Information Systems (AIS) Security Program*, defines responsibilities for protecting FDIC AISs against data loss, intrusions, and destructive or abusive behavior from internal or external sources. Additional guidance, along with a description of computer security incidents, is available on the Division of Information Technology (DIT) webpage under the "Security Incident Reporting" section.

- **National Institute of Standards (NIST) guidance**, including National Institute of Standards (NIST) Special Publication 800-61, *Computer Security Handling Incident Guide*, which provides guidance on incident handling and reporting; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,* which catalogs security controls for Federal information systems and provides a Risk Management Framework that addresses security control selection for federal information systems in various areas including but not limited to incident response; and NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of PII*, which provides guidance on how to develop an incident response plan to handle a breach involving PII.

- **Federal Information Processing Standards (FIPS),** including *Minimum Security Requirements for Federal Information and Information Systems* (FIPS 200)*, Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199*),* which provides standards to Federal agencies for establishing minimum security requirements and controls and assigning an impact level to all information and information systems.

# 2 KEY TERMINOLOGY

This section defines and provides examples of key terminology used in this manual. For a full listing of terminology used in this guide, see **Appendix N, *Glossary of Terms and Definitions.***

## *2.1 What is Sensitive Information (SI)?*

Sensitive information (SI) includes any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. In general, sensitive information is information that contains an element of confidentiality. As used in this guide, SI encompasses both agency and business sensitive information and personally identifiable information, as defined below.

- **Agency and Business Sensitive Information (BSI)** refers to identifying information about the Corporation, a government agency, a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices or other crimes, such as bank account information, trade secrets, confidential or proprietary business information. Commercial information is not confined to records that reveal basic commercial operations, but includes any information in which the submitter has a commercial interest, and may include information submitted by a nonprofit entity. Other terms for BSI that must be protected from disclosure are: "confidential business information," "business identifiable information," "confidential commercial information," and "proprietary information."

- **Personally Identifiable Information (PII)** refers to any information about an individual maintained by FDIC which can be used to distinguish or trace that individual's identity, such as their full name, home address, e-mail address (non-work), telephone numbers (non-work), social security number (SSN), driver's license/state identification number, employee identification number (EIN), date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number), medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.

*Table 2.1.1 – Examples of Sensitive Information (SI)*

| **Type of Information** | **Definition** | **Examples** |
|---|---|---|
| Agency Sensitive Information | Any information under the care of FDIC where its inappropriate release could harm or embarrass the FDIC, the financial institutions we supervise, or entities/businesses to *which* the information pertains. Business Sensitive Information (defined below) is considered a subset of agency sensitive information. | • Bank examination and bank closing information.<br>• Information which could assist someone in criminal activity (such as government credit card numbers or schematics of buildings).<br>• Attorney work product or attorney-client information.<br>• Certain law enforcement information or information about pending litigation.<br>• Agency confidential or proprietary information that could disadvantage the agency in an ongoing negotiation, or confuse the public about future plans.<br>• Security management information<br>• Information related to FDIC's network or information technology that could be misused by malicious entities (e.g., IP addresses, server names, firewall rules, encryption and authentication mechanisms, and network architecture pertaining to FDIC)<br>• Pre-decisional planning and budgeting documents<br>• Continuity-of-operations information |

| | | |
|---|---|---|
| Business Sensitive Information | A subset of agency sensitive information that includes information under the due care of a Federal agency that is sensitive to businesses or corporations. Business or commercial information is not confined to records that reveal basic commercial operations, but includes any information in which the submitter has a commercial interest, and may include information submitted by a nonprofit entity. Other terms for Business Sensitive Information that must be protected | • Trade secrets<br>• Manufacturing processes, operations or techniques<br>• Business financial information<br>• Amount or source of any profits, losses or expenditures<br>• Confidential or proprietary information provided to the Corporation by companies, organizations, or other agencies |
| Personal (Personally Identifiable Information) | Any information about an individual maintained by FDIC which can be used to distinguish or trace that individual's identity, or any other personal information which is linked or linkable to an individual. | • Name<br>• Home Address<br>• Telephone Number (Non-Work)<br>• Email Address (Non-Work)<br>• Date and Place of Birth<br>• Social Security Number (SSN)<br>• Mother's Maiden Name<br>• Customer Financial Information<br>• Medical and Health Information<br>• Photograph<br>• Biometric Identifiers<br>• Criminal or Employment Information |

A non-exclusive inventory of critical agency-sensitive information is referenced in **Appendix A** of this guide.

## *2.2 What Is an Incident?*

An incident refers to an adverse event or situation that poses a threat to the integrity, availability or confidentiality of FDIC's information systems, network or data. This definition applies to electronic and non-electronic data. It includes both intrusions from outside the Corporation and misuse from within the Corporation. An incident may result in the following:

- Failure of FDIC information security or privacy controls;
- Waste, fraud, abuse, loss, damage or compromise of FDIC systems, assets or information; and/or
- Violation or imminent threat of violation of FDIC policies for privacy, security, IT, and/or data protection.

Table 2.2.1 contains the various types of incidents that may threaten FDIC's IT infrastructure, systems or data.

| **Name** | **Definition** |
|---|---|
| **Unauthorized Access** | When an individual or entity gains logical or physical access without permission to FDIC's network, systems, applications, assets, data, or other resources. |
| **Denial of Service (DoS)** | An attack that successfully prevents or impairs the normal authorized functionality of FDIC's network, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. |
| **Malicious Code** | Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus (AV) software. |
| **Improper Usage or Policy Violation** | When an FDIC employee, contractor, intern or other person violates acceptable computing policies and/or data protection policies. |
| **Suspected Loss** | An incident that involves a suspected loss, theft or compromise of agency or |

| | |
|---|---|
| **or Compromise of BSI** | business sensitive information (BSI) that occurred as a result of unauthorized access, malicious code, failure of privacy/security controls, or improper (or inappropriate) use or disclosure. Such incidents can occur in electronic, verbal or hardcopy form. |
| **Suspected Breach of PII** | An incident that involves the potential or suspected loss, theft, or breach of personally identifiable information (PII), whether in electronic, verbal or hardcopy form. (Suspected PII incidents can be resolved by confirmation of a non-PII determination.) |

***Table 2.2.1 – Incident Categorization***

## *2.3 What Constitutes a Data Breach?*

For purposes of this guide, a data breach is defined as an incident in which FDIC sensitive information, including BSI and/or PII, has been lost, compromised, acquired, disclosed, or accessed without authorization, or any similar incident where persons other than authorized users and for other than authorized purposes have access or potential access to sensitive information. This definition applies to electronic and non-electronic data. It includes both intrusions from outside the Corporation and misuse from within the Corporation.

Data breaches can take many forms, including but not limited to:

- Adversary or hostile actor gaining access to data through a malicious attack or social engineering;
- Lost, stolen or compromised electronic records, electronic equipment, or hardcopy/physical records containing BSI or PII;
- Verbal disclosures of BSI or PII;
- Employee/contractor negligence (e.g., sharing data with an unauthorized person; leaving a password to a system containing sensitive data in a publicly accessible location; technical staff misconfiguring a security service or device, etc.); or
- Policy violation or system failure.

As illustrated by these examples, data breaches may include both physical security incidents and computer security incidents[4], when such incidents involve the loss, theft or compromise of sensitive information (BSI and/or PII). In addition, a data breach could result from a verbal disclosure of sensitive information, whether intentional or unintentional. Refer to **Appendix B** for specific examples and descriptions of data incidents that should be reported immediately upon discovery or detection.

[4] A computer security incident is an event that threatens the security of the FDIC Automated Information System (AIS), which includes FDIC's computers, mainframe, networks, software and associated equipment, and information stored or transmitted using that equipment. Computer security incidents involving BSI and/or PII are handled in accord with this guide, as well as FDIC Security Protection Engineering Section (SPES) standard operating procedures (SOPs).

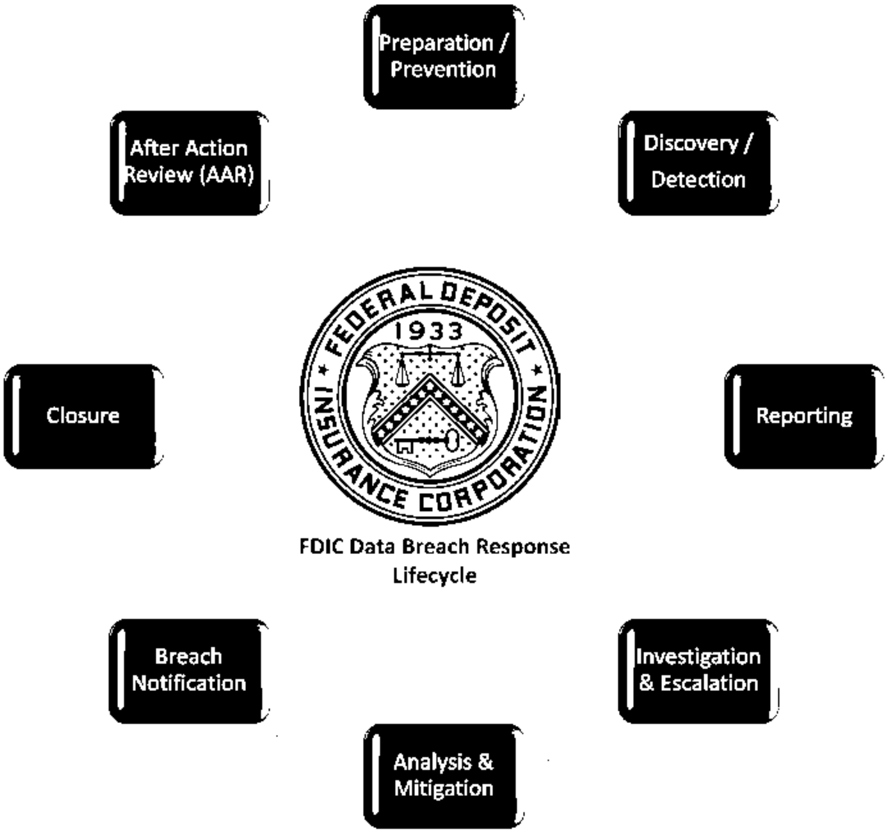
# 3 OVERVIEW OF FDIC BREACH RESPONSE LIFECYCLE

As outlined below, there are eight (8) core stages of the FDIC data breach handling or response process. The overarching objective of this 8-stage process is to ensure that FDIC responds in a timely and effective manner to known or suspected data breaches, in order to protect FDIC information and assets, as well as to limit harm to affected individuals and entities.

**Stages of the Data Breach Response Lifecycle**

| # | Stage | Description |
|---|---|---|
| 1 | **Preparation/Prevention** | Preparing for incidents by establishing a formal incident response capability and providing targeted training to employees, contractors and incident response team members. Preventing incidents through the implementation of sufficient administrative, physical and technical controls to safeguard FDIC information and the systems and facilities wherein the data resides. |
| 2 | **Discovery/Detection** | Discovery or detection of the incident by an end user, third-party, or automated security scan or monitoring tool. |
| 3 | **Reporting** | Reporting known and suspected breaches within OMB-mandated and United States Computer Emergency Readiness Team (US-CERT) established timeframes. |
| 4 | **Data Collection, Investigation & Escalation** | Collecting and documenting facts about the circumstances of the incident, including but not limited to the cause of the incident, type and nature of data involved, the number of individuals/entities affected, etc. Notifying and escalating the incident to the appropriate internal and external resources for a quick and effective response. |
| 5 | **Analysis & Mitigation** | Analyzing and determining the potential impact / risk of harm that the incident poses to the Corporation and affected individuals/entities. Determining an appropriate course of action designed to limit the potential harm posed by the incident.<br>Implementing an appropriate course of action to mitigate the incident and limit harm to the Corporation and affected individuals/entities. |
| 6 | **External Breach Notification** | Notifying affected individuals and entities, as appropriate, in a timely manner and consistent with relevant Federal and state breach notification requirements. |
| 7 | **Closure** | Preparing an Incident Close-Out Report and notifying the Computer Security Incident Response Team (CSIRT) to officially close the incident. |
| 8 | **After Action Review (AAR) / Lessons Learned** | Conducting post-closure activities, such as identifying "lessons learned" and metrics to improve the overall efficiency and effectiveness of the incident response process. Lessons learned and findings identified during the AAR feed into Step 1 (Preparation/Prevention). |

From a high-level, the FDIC's data breach management process is cyclical, with each stage feeding into the next, as illustrated in the figure below. However, in practice, the stages of the incident handling process are performed in the order of priority as warranted by the circumstances of the incident. In some cases, certain incident handling stages and sub-steps may not apply or may need to be performed in parallel. For example, incident assessment and mitigation activities (Step 5) could commence, while investigation and documentation activities of the preceding step (Step 4) continue. Thus, the potential for multitasking incident steps and sub-steps is entirely possible and ultimately dependent on the nature of the incident.



FDIC Data Breach Response Lifecycle

Each stage in the lifecycle, along with the roles and responsibilities of key participants, are described in greater detail in the subsequent sections.

# 4 ROLES AND RESPONSIBILITIES

The following section describes the roles and responsibilities of key actors involved in the FDIC data breach response process.

(b)(2),(b)(5)

| ROLES | RESPONSIBILITIES |
|---|---|
| User[5] | [redacted] |
| Immediate Supervisor or Oversight Manager | [redacted] |

[5] Note: Not all user requirements listed in Section 4 are applicable to outsourced services providers, office visitors and government agencies and organization with authorized access to FDIC data. The key requirement applicable to said users is to immediately report the loss, theft or compromise of FDIC sensitive information to the FDIC. Additional requirements for protecting FDIC-provided data are outlined in applicable contractual and/or sharing agreements between the entity/agency and FDIC. For example, FDIC outsourced service providers are required contractually to implement an incident response capability and to immediately report the loss, theft or compromise of FDIC sensitive information to the FDIC Help Desk/CSIRT. Providers are also required to protect sensitive information in accordance with the information security and privacy requirements stipulated in their contracts and Confidentiality Agreements with FDIC. However, completion of FDIC's annual Information Security and Privacy Awareness Training is not contractually required; although, a similar or comparable training is encouraged.

[6] See footnote above.

(b)(2),(b)(5)

[redacted]

(b)(2),(b)(5)

| ROLES | RESPONSIBILITIES |
|---|---|
| **FDIC Help Desk** | [redacted] |
| **Computer Security Incident Response Team (CSIRT)** | [redacted] |
| **Divisional Incident Response Point of Contact (Divisional IR POC)** | The Divisional ISM serves as the primary IR POC for his/her Division or Office. Additional Divisional IR POCs may also be designated to assist the ISM with investigating and handling the incident. For example, members of the Divisional IT Security Group, Divisional Internal Review Group, or other Divisional staff members may be authorized by the Division/Office Director (or designee) to serve as the primary or secondary Divisional IR POCs. The Divisional IR POC is responsible for participating in the development and execution of a corporate response plan in the event of loss or compromise of BSI and/or PII. |

| ROLES | RESPONSIBILITIES |
|---|---|
| **Divisional Incident Response Team (Divisional IRT)** | The Divisional IRT follows the Division IR POC's leadership and works under the Divisional ISM's direction. The Divisional IRT is responsible for coordinating with CSIRT, the ISPS Incident Lead, and the DBMT in the event of a loss or compromise of sensitive information (BSI and/or PII). |
| **Divisional Information Security Manager (ISM)** | The Divisional ISM is an FDIC employee assigned to ensure divisional compliance with FDIC Security circulars, implement business specific security practices, and serve as the primary liaison between the FDIC Information Security and Privacy Staff (ISPS) and the ISM's Division/Office. The ISM is responsible for:<br>• Helping to ensure that sensitive information, including business and personally identifiable information is adequately protected through their participation in FDIC's Information Security Risk Management Program;<br>• Serving as the primary Divisional IR POC and coordinating with any secondary or supplemental Divisional IR POC(s) in the Regions, Field, or Headquarters;<br>• Assisting CSIRT and the ISPS Incident Lead in collecting and documenting facts related to the incident upon request;<br>• Working with the ISPS Incident Lead to perform an impact assessment of the incident; and<br>• Assisting in the development and execution of a corporate response plan in the event of loss or compromise of BSI and/or PII. |
| **Information Security and Privacy Staff (ISPS) Incident Lead** | The ISPS Incident Lead is an FDIC employee assigned to ensure that any known or suspected breaches that involve BSI and/or PII are appropriately managed to closure. The Privacy Program Manager (PPM) will serve as and/or designate a Privacy/Data Protection Specialist to serve as the ISPS Incident Lead in the event of a data breach. The ISPS Incident Lead is responsible for:<br>• Evaluating the Security Incident Report provided by CSIRT and any additional facts gathered by the Divisional ISM/Divisional IR POC(s) to evaluate the nature of the incident;<br>• Assisting and providing guidance to the Divisional ISM/Divisional IR POC(s) in investigating and taking appropriate remedial actions;<br>• Coordinating with the Divisional ISM/Divisional IR POC(s) to perform an impact assessment of the incident and prepare a recommended course of action; and<br>• Managing the incident to closure or convening the Data Management Breach Team (DBMT), as appropriate, and facilitating and managing all activities of the DBMT;<br>• Keeping the CIO/CPO, CISO, and PPM duly apprised of the status of incidents as needed;<br>• Review and authorize the Divisional ISM's incident closure recommendation for incidents involving BSI or PII;<br>• Preparing and submitting a Final Breach Close Out Report / Summary to the CIO/CPO, CISO and PPM upon closure of the incident; and<br>• Facilitating an after action review (AAR) to determine lessons learned. |
| **Chief Information Officer (CIO)/ Chief Privacy Officer (CPO)** | The CIO/CPO serves as the Senior Agency Official for Privacy (SAOP) for the Corporation. The CIO/CPO is primarily responsible for the Corporation's privacy and data protection policy. In the event of a loss or compromise of SI (including BSI and/or PII), the CIO/CPO or designee is responsible for:<br>• Participating in the DBMT as requested;<br>• Reviewing and approving the DBMT's recommended course of action, including external breach notification letters and offers of credit monitoring; and<br>• Notifying the Executive Office (EO) and Chief Risk Officer of the recommended course of action, including external data breach notification and communications, if applicable. |

| ROLES | RESPONSIBILITIES |
|---|---|
| **Chief Information Security Officer (CISO)** | The CISO serves as principal advisor for the Corporation's IT security and privacy programs. The CISO is responsible for developing the Corporation's security policy, and establishing and managing the Corporation's Privacy Program.<br>In the event of a loss or compromise of SI, the CISO participates in the DBMT as requested and helps advise the CIO/CPO on whether a breach notification or any further actions are required. The CISO also participates in the after action review (AAR) as needed to provide insight and help identify security control enhancements, process improvements and other lessons learned to improve the overall incident response capability. Additionally, the CISO (or designee) periodically tests and evaluates the effectiveness of information security/privacy incident handling policies, procedures and practices. |
| **Chief Risk Officer (CRO)** | The CRO directs the affairs of the Office of Corporate Risk Management and strategically manages a comprehensive risk management program to address the Corporation's emerging and crisis-related risks. The CRO also serves as a strategic adviser to the Chairperson, the Board of Directors, and Division and Office leadership in centrally managing risks across the Corporation and ensuring that sound risk management principles are used in executive decision making and strategy development.<br>In the event of a data incident or breach, the CRO (or designee):<br>• Participates in the DBMT as requested;<br>• Reviews and provides feedback on the incident risk assessment supporting the recommended course of action identified by the DBMT;<br>• Escalates incidents that have significant potential impact to the Corporation to the Executive Risk Committee (ERC), as necessary; and<br>• Communicates the ERC decision and guidance to the DBMT. |
| **Privacy Program Manager (PPM)** | The PPM advises the Corporation CIO/CPO and CISO in the development, daily operation, and management of the FDIC Privacy Program. These efforts include the development, implementation and maintenance of, and adherence to, the FDIC policies and procedures related to privacy and data protection. The PPM leads initiatives to strengthen information privacy protections. In the event of a loss or compromise of BSI and/or PII, the PPM is responsible for:<br>• Designating or serving as the ISPS Incident Lead;<br>• Providing advice and leadership to the Divisional ISM/IR POC(s), ISPS Incident Lead (if other than PPM), and DBMT as needed in assessing the potential likelihood and magnitude of harm caused by the breach (note: this responsibility may be designated to the Head of the affected Division or Office);<br>• Coordinating with the CISO to advise the CIO/CPO regarding whether a breach notification, either internal or external, should be made;<br>• Overseeing the notification process;<br>• Participating in the after action review (AAR) and lessons learned;<br>• Assisting the ISPS Incident Lead with preparing and submitting a Final Breach Close Out Report/Summary to the CIO/CPO upon closure of the incident; and<br>• Maintaining and overseeing updates to this guide, in coordination with the DBMT, at least annually or whenever there is a material change. |
| **Data Breach Management Team (DBMT)** | The DBMT is led by the ISPS Incident Lead with members who are authorized representatives from the Legal Division, Affected Division/Office, IT Security and Privacy, and Office of Communications, as applicable. Additional FDIC Program Area Specialists may be asked to participate in the DBMT as appropriate and germane to the incident, such as the Office of Legislative Affairs, Office of Inspector General, |

| ROLES | RESPONSIBILITIES |
|---|---|
| | Internal/External Ombudsman, and SEPS Physical Security. The DBMT is responsible for:<br>• Reviewing and approving the incident risk analysis/impact assessment prepared by the ISPS Incident Lead and Divisional ISM (the impact assessment describes the likely risk of harm caused by a breach of SI and the level of risk, based on the CSIRT report, and proposes whether notification or other actions are required.);<br>• Identifying any additional resources or mitigation actions required to properly respond to the incident;<br>• Managing the approved course of action; and<br>• At the direction of the PPM or designee, reviewing FDIC implementation of this guide at least annually to capture ongoing changes to resources and business environment.<br>*Note: Refer to Section 5 for more information about the DBMT.* |
| **Affected FDIC Division or Office/Data and Business Owners** | This is the division or office that owns or maintains the BSI and/or PII that was lost, stolen or otherwise compromised. The affected division/office is responsible for:<br>• Working under direction of the ISPS Incident Lead and the Data Breach Management Team to mitigate the incident;<br>• Identifying the nature and extent of the breach and associated data loss, and<br>• Paying the costs for labor associated with the work of notification to the affected persons and/or entities as well as cost of credit monitoring[8]. |
| **FDIC Divisional/Office Database Administrator (DBA)** | The DBA is the individual responsible for the installation, configuration, administration, monitoring and maintenance of systems/databases for the Division/Office. In the event of a data incident or breach, the DBA analyzes the system breach and determines which records may be affected. |
| **Executive Office** | In the event of a data breach, the Executive Office is responsible for providing concurrence or feedback on the recommended course of action identified by the DBMT. |
| **Legal Division** | In the event of a loss or compromise of BSI and/or PII, the Legal Division is responsible for:<br>• Coordinating with the DBMT in ensuring a corporate response plan is successfully executed in compliance with federal laws and regulations;<br>• Reviewing and approving the notification letter drafted by the affected division/office; and<br>• Coordinating with the Office of Communications in responding to FOIA inquiries. |
| **FDIC Office of Inspector General (FDIC OIG)** | The FDIC OIG is an independent unit that conducts audits, investigations, and other reviews of the Corporation's programs and operations, including the Privacy Program. In the event of a loss or compromise of BSI and/or PII, particularly if there is suspected violation of criminal law, the OIG will be notified by the CSIRT so that the OIG can conduct an investigation as needed and/or cooperate with the FBI or other law enforcement agencies. The OIG will also participate in the DBMT as requested. |

(b)(2),(b)(5)

[redacted]

| ROLES | RESPONSIBILITIES |
|---|---|
| **Division of Administration, Acquisitions Services Branch (ASB)** | ASB is responsible for procuring goods and services on behalf of the Corporation. ASB Contracting Officers (COs) and other ASB personnel work with Oversight Managers (OMs) and Technical Monitors (TMs) to monitor contractor performance, including all security requirements set forth in the contract.<br>In the event of a data incident involving a contractor or vendor, ASB will participate in the DBMT as requested; provide guidance on any contracting issues raised by the incident; and help advise on and implement any recommended courses of action involving contractor noncompliance or other contracting issues identified by the DBMT. |
| **Division of Finance (DOF), Corporate Management Control (CMC)** | The CMC manages internal controls and operational risks by maintaining partnerships with the Divisions and Offices, providing training, and addressing identified internal control deficiencies.<br>In the event a loss or compromise of SI points to a systemic risk that is not sufficiently addressed, the CMC will work with the DBMT in mitigating that risk. |
| **FDIC Office of Legislative Affairs (OLA)** | The FDIC Office of Legislative Affairs serves as the Corporation's congressional liaison and closely monitors and responds to legislation important to the Corporation. In the event of a loss or compromise of BSI and/or PII, the OLA is responsible for:<br>• Serving as a central POC in notifying appropriate committees and Members of the Congress about the incident as well as in responding to requests from various Congress committees/members or their staff about the incident; and<br>• Collaborating with the DBMT. |
| **FDIC Office of Communications (OCOM)** | OCOM acts as the Corporation's central contact point for responding to media inquiries and initiating press contacts. In the event of a loss or compromise of BSI and/or PII, OCOM is responsible for:<br>• Organizing press conference, if required;<br>• Participating in the DBMT if requested;<br>• Responding to media inquiries and initiating press release about the breach; and<br>• Coordinating with Legal Division in responding to FOIA inquiries regarding the breach. |
| **FDIC Ombudsman (Internal & External)** | The Office of the Ombudsman ("OO" or "External Ombudsman") is an independent, neutral, and confidential resource and liaison for the banking industry and general public to facilitate the resolution of problems and complaints against the FDIC in a fair, impartial, and timely manner. The OO provides prompt and meaningful feedback to influence positive change.<br>The Internal Ombudsman supports the mission of the FDIC by seeking resolution of work-related questions and concerns raised by all levels of management and staff.<br>In the event of a data breach, the Ombudsman (Internal and/or External) will participate in the DBMT as requested; and provide facilitation and problem resolution services for complaints or issues that may arise from a reported incident. |

(b)(2),(b)(5)

(b)(2),(b)(5)
(b)(2),(b)(5)
)(2),(b)(5)

| ROLES | RESPONSIBILITIES |
|---|---|
| **FDIC Call Center** | The FDIC Call Center is the primary telephone point of contact for the banking industry and the general public. Callers reach the Call Center through a toll-free or direct phone number ([redacted]) or a TDD ([redacted] or [redacted] [redacted].) In the event of a loss or compromise of BSI and/or PII, the Call Center is responsible for:<br>• Answering questions from affected individuals based on scripts provided by the ISPS Incident Lead and DBMT;<br>• Transferring questions deemed by a Call Center agent to be of a "technical nature" to a DBMT subject matter expert (SME); and<br>• Working with the ISPS Incident Lead and DBMT to update the scripts to include new evolving issues or scenarios. |
| **Local Law Enforcement Agency (LLEA)** | Local Law Enforcement Agency (LLEA) is the local Police Office for the district in which the loss or theft of FDIC equipment, records or other assets takes place. Upon receiving a report about the loss/theft of equipment or other assets from the user, the LLEA is responsible for:<br>• Running the investigation and informing the user about the investigation findings/results; and<br>• Coordinating with other law enforcement agencies (the FBI, State Police Department, etc.) in conducting the investigation. |
| **Security Emergency Preparedness Section (SEPS), Physical Security Unit** | The Security Emergency Preparedness Section (SEPS) of the Corporate Services Branch, Division of Administration (DOA), of the FDIC is responsible for personnel security, physical security, emergency operations, transportation, business continuity and safety of all Corporation personnel. In the event of a breach of SI, including BSI and/or PII, the SEPS Physical Security Unit is responsible for:<br>• Investigating the physical incident if it took place within FDIC territory;<br>• Recording the incident into the FDIC Incident Reporting Investigation Management System (IRIMS); and<br>• Reporting the incident results/fact findings to the CIO/CPO, CISO, and PPM or authorized designees. |
| **Security Protection and Engineering Section (SPES)** | SPES is responsible for ensuring that operational safeguards are in place which include providing multi-platform security in areas of access controls, security awareness and training, application and support system security controls, operational support for Public Key Infrastructure (PKI), and monitoring and reporting. SPES personnel [redacted] [redacted] are responsible for immediately reporting to CSIRT any computer security incidents identified during the course of investigations or normal business activities. |
| **The United States Computer Emergency Readiness Team (US-CERT)** | Established in 2003, the US-CERT's mission is to protect the nation's internet infrastructure. US-CERT coordinates defense against and responses to cyber-attacks across the nation. In the event of a loss or compromise of BSI and/or PII, the US-CERT is responsible for:<br>• Notifying appropriate officials in the executive branch of the government about the breach incident;<br>• Coordinating communications of the breach incident with other agencies; and<br>• For PII incidents, distributing to designated officials in the agencies and elsewhere, a monthly report identifying the number of confirmed breaches of PII and making available a public version of the report. |

*Table 4.1: Roles and Responsibilities in the Data Breach Response Process*

# 5 FDIC DATA BREACH MANAGEMENT TEAM (DBMT)

The FDIC has established the Data Breach Management Team (DBMT) to manage FDIC's response in the event of an actual or suspected data breach involving agency or business sensitive information (BSI) and/or personally identifiable information (PII). The role of the DBMT is to:

- Review and verify the incident risk assessment, in terms of the level of harm posed to affected individuals/entities, the financial sector (if applicable), and the Corporation;
- Determine and manage the appropriate course of action to respond to the breach and mitigate any harm; and
- Recommend appropriate external breach communications and notification, including notification to affected individuals, banks, or other entities to the CIO/CPO (or designee) for approval.

Additionally, the DBMT, at the direction of the PPM or designee, shall initiate and oversee a complete review and update of these procedures, at least annually, to capture ongoing changes to resources and business environment.

## *5.1 DBMT Leadership*

The DBMT is convened, facilitated, and managed by the Information Security and Privacy Staff (ISPS) Incident Lead, who is an FDIC employee designated to manage the incident on behalf of ISPS. The Privacy Program Manager (PPM) will serve as and/or designate an ISPS staff member to serve as the ISPS Incident Lead.

## *5.2 DBMT Membership*

The ISPS Incident Lead is responsible for determining which members should be invited to participate in the DBMT on a "need to know" basis and as warranted by the circumstances of the data breach. (Refer to the next section for guidance on invoking the DBMT.) The makeup of the DBMT **will vary depending on the circumstances of the potential data breach**.

With this in mind, the DBMT **may** include the following representatives:

- Chief Information Officer (CIO) / Chief Privacy Officer (CPO) and/or Designee
- Chief Information Security Officer (CISO) and/or Designated IT Security Specialists
- Privacy Program Manager (PPM) and/or Designated Privacy Specialists
- Information Security and Privacy Staff (ISPS) Incident Lead
- Legal Division, Deputy General Counsel, and/or Designee
- Office of Communications (OCOM) Director and/or Designee
- Chief Risk Officer (CRO) and/or Designee
- Affected Division/Office Director and/or Designee
- Divisional Information Security Manager (ISM) / Divisional Incident Response POC(s) from the **Affected** Division/Office
- Appropriate FDIC Program Area Specialists (**Situational Dependent – See list of examples below**.)

Following are examples of FDIC Program Area Specialists who may be asked to participate in the DBMT as warranted by the circumstances of the data breach:

- Appropriate Technical Staff

- DOA Security and Emergency Preparedness Section (SEPS) Assistant Director and/or Designee (if loss/theft occurs on FDIC premises, or if incident otherwise involves physical security issues or implications requiring SEPS' attention)
- DOA Acquisitions and Servicing Branch (ASB) Assistant Director and/or Contracting Officer (CO) and/or Oversight Manager (OM) (if incident involves a contractor, vendor, or outsourced provider, or if incident otherwise triggers contracting issues or implications)
- Division of Finance (DOF), Corporate Management Control (CMC) (if incident points to a systemic risk that is not sufficiently addressed)
- Office of Inspector General (OIG) Special Agent-In-Charge and/or Designee (if OIG criminal investigation or involvement is needed; for example, if criminal activity is suspected)
- Office of Legislative Affairs (OLA) Director and/or Designee (if incident involves legislative and/or inter-governmental issues)
- External or Internal Ombudsman and/or Designee (if incident involves a complaint/issue or matter that falls within the scope/mission of the External or Internal Ombudsman)

# 6 DATA BREACH RESPONSE QUICK GUIDE

The following quick reference guide provides the key steps and timeframes for completing each stage of the FDIC's data breach response lifecycle, with focus on the steps involved from reporting onward.

(b)(2),(b)(5)

[redacted]

(b)(2),(b)(5)

[redacted]

[9] Incidents may also be reported to the FDIC Help Desk/CSIRT via email at [redacted] (b)(2),(b)(5)

Page 097 of 157

(b)(2),(b)(5)

| | |
|---|---|
| | Mailbox and the Divisional ISM. |

# 7 DATA BREACH RESPONSE PROCEDURES

This section provides detailed procedures for responding to data breaches, from prevention and discovery through closure and after action review (AAR).

## *7.1 Preparation & Prevention*

The first step in the incident response process is taking appropriate actions to prepare for and prevent a data breach from occurring. One important component of FDIC's efforts to prevent breaches is user awareness and training as explained in Section 7.1.1. Refer to **Appendix C** for additional measures that FDIC takes to prevent data breaches.

### 7.1.1 Awareness and Training

On an annual basis, all FDIC employees and contractors must complete the Corporate Information Security and Privacy Awareness training, which tests and affirms their understanding of their responsibilities for safeguarding agency-sensitive information and PII, and for immediately reporting the loss, theft or compromise of such data in accord with the procedures outlined in this guide. In addition, the Corporation will provide targeted, role-based training to key parties involved in the incident response process (refer to the **Roles and Responsibilities Section** of this procedural guide) on an annual basis. This training will be provided in the form of mandatory privacy/security clinics and data breach simulation/tabletop exercises. Refer to **Appendix C** for more information about awareness and training activities to help prevent breaches.

## *7.2 Incident Detection/Discovery*

There are several ways in which a data breach may be discovered or detected, the most common being: (a) user[10] detected, (b) third-party[11] detected, or (c) system or security[12] detected. Whether a user discovers a breach firsthand or is alerted to it by a third-party source, the user is responsible for reporting the incident immediately, following the procedures outlined below. For help in identifying or detecting a breach, review **Appendix B** which provides examples of various types of reportable data incidents.

## *7.3 Incident Reporting*

(b)(2),(b)(5)

[redacted]

[10] For purposes of this guide, a user refers to an FDIC employee, contractor, intern, vendor, outsourced provider, or other individual (e.g., non-FDIC government employee) with authorized access to FDIC data. A user detected incident refers to when an individual user discovers the loss, theft or compromise of data, in any medium, belonging to him/her or to another user.

[11] A third-party detected incident refers to when a third-party (non-FDIC) source detects an incident involving FDIC sensitive information.

[12] A security or system detected incident refers to when FDIC IT Security personnel detect the loss, theft or compromise of FDIC data via computer monitoring tools, automated security scans, data loss prevention capabilities, etc.

(b)(2),(b)(5)

[redacted]

(b)(2),(b)(5)

[redacted]

## 7.4 *Incident Investigation & Escalation*

Once an incident has been discovered and reported, appropriate action must be taken to gather all pertinent information and document everything that is known about the suspected or confirmed breach, including but not limited to: who discovered/reported the incident, what type of information or equipment was lost/stolen/accessed, how the loss occurred, what systems are affected, etc. This information is necessary to assess the nature and scope of the incident.

Refer to 7.4.1 and 7.4.2 for an overview of the main actors and steps that are involved in the investigation and escalation stage.

### 7.4.1 Incident Intake and Documentation

(b)(2),(b)(5)

[redacted]

### 7.4.2 FDIC CSIRT Incident Fact Gathering and Escalation

(b)(2),(b)(5)

[redacted]

Page 101 of 157

(b)(2),(b)(5)

Page 102 of 157

(b)(2),(b)(5)

(b)(2),(b)(5)

[redacted]

### 7.4.4 ISPS Incident Assistance & Oversight

Upon being alerted of an incident that involves sensitive information (BSI and/or PII), the PPM will serve as or designate an ISPS Incident Lead to follow up with the affected Division/Office ISM. The ISPS Incident Lead will notify CSIRT and the Divisional ISM that he/she has been assigned to the incident and will coordinate with the Divisional ISM to ensure appropriate actions are being taken to investigate and handle the incident, and to perform an incident risk analysis (impact assessment) as detailed in the next section. The ISPS Incident Lead will serve as the final approver of the Incident Risk Analysis (IRA) and make a determination about the final risk level (high, medium, low) and breach/non-breach designation for each incident.

## *7.5 Incident Risk Analysis & Mitigation*

After CSIRT and the affected Division/Office have completed their preliminary investigation, the following activities will be performed, depending upon the nature and type of data involved in the incident.

**Non-Breaches**

For incidents where sensitive information (BSI and/or PII) has NOT been breached, or where there is a low or non-existent risk of harm, CSIRT will follow internal procedures for eradicating/ containing the incident and notifying applicable resources.. Additionally, ISMs/Div IR POCs should follow their standard procedures for investigating these types of incidents; determining and educating the user about any applicable policy violations; and completing an Incident Risk Analysis (IRA) form (Appendix L). As applicable, the ISM/Div IR POC may leverage a pre-populated IRA for incidents that ISPS has assessed and pre-determined to be non-breaches. Examples of such incidents are:

- **Open network shared folders ("open shares")** that are immediately locked down and have not been accessed by unauthorized parties or for unauthorized purposes, based on available information; and
- **Encrypted devices** (e.g., laptops, blackberries, USB devices, etc. that have been encrypted utilizing an FDIC-approved encryption protocol) that are wiped or recovered immediately and do not appear to have been targeted for the data contained on said devices; etc.).

**Potential / Actual Breaches**

For incidents that involve an actual or potential breach of sensitive information (BSI and/or PII), the Divisional ISM/IR POC(s) will coordinate with the ISPS Incident Lead to conduct an initial risk analysis (impact assessment) of the incident and document the findings in the Incident Risk Analysis (IRA) form (Appendix L). The primary objectives of the risk analysis are to:

1. Determine the potential severity/likely risk of harm posed by the incident based on an evaluation of the five factors set forth below;
2. Decide whether the entire or a smaller, specialized Data Breach Management Team (DBMT) should be invoked;
3. Assess whether notification may be warranted; and
4. Identify an appropriate course of action and next steps to mitigate the risk of harm.

The Incident Risk Analysis is conducted using the methodology described below.

Refer to **Appendix K and Appendix L** for more information and a detailed guide for conducting an incident risk analysis using the 5-factor methodology.

## 7.5.1 Incident Risk Analysis Methodology

The Corporation uses a five (5) factor risk analysis methodology (depicted below) to assess the likely risk of harm caused by an incident and determine the appropriate course(s) of action. The FDIC's risk management approach is based on Office of Management and Budget (OMB) guidance[17] and National Institute of Standards and Technology (NIST) risk assessment guidelines, which utilize the impact levels of Low, Moderate and High to rate the potential harm that could result if data were inappropriately accessed, used or disclosed.

[17] Refer to OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, issued on May 22, 2007, which is available at: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

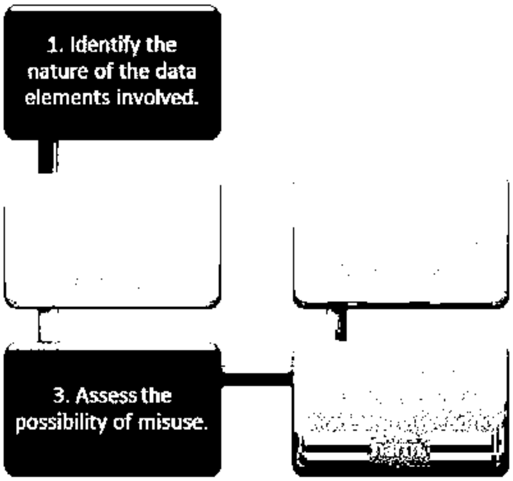

1. Identify the nature of the data elements involved.
3. Assess the possibility of misuse.

*Figure 6.5.1.1. 5-Factor Incident Risk Analysis*

## 7.5.2 Potential Impact/Risk Determination

Using the above methodology, the ISPS Incident Lead and Divisional ISM/IR POCs will assess each of the five factors (identified above) in relation to the specific incident. They will then balance the five factors collectively and assign an overall risk determination level (Low, Moderate or High) to the incident. In assessing the five factors, the following questions should be considered:

- What is the likely risk of harm?
- Was the loss intentional?
- Was the compromised data deliberately targeted?
- What was the sensitivity level of the data involved in the incident? For example:
    - Was sensitive bank exam, charter, or closing information compromised?
    - Was sensitive personal information, financial information (e.g. credit card numbers), or Social Security Numbers lost/stolen or otherwise compromised?
- In what medium (paper, email, thumb drive, system, etc.) was the data maintained, and what associated controls (encryption, password-protection, etc.) were in place?
- Could the lost/stolen/compromised information be used to perform identity theft or cause other harm to entities or individuals?
- Could the lost/stolen/compromised information damage the reputation or cause a financial loss to entities or individuals?
- How many individuals or parties were affected?
- Are the identities of the affected individuals or parties known?

The more significant the potential harm, the more time-critical the notification of affected individuals or parties becomes. In cases where there is little or no risk of harm, notification might create unnecessary concern and confusion. Under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Refer to **Appendix K and Appendix L** for more information and a detailed guide for conducting an incident risk analysis using the 5-factor methodology.

### 7.5.3 Incident Risk Analysis (IRA) Template

The Divisional ISM/IR POC will document the findings of the investigation and the impact assessment using the Incident Risk Analysis (IRA) template provided in Appendix L of this Guide. The Divisional ISM/IR POC should email the completed, draft IRA, along with any supporting documentation, to the ISPS Incident Lead, copying the Privacy Incidents mailbox. Note that for high-risk incidents, a timeline of key events and a summary of the investigation should also be drafted by the ISM/IR POC and be included in or attached to the IRA. The ISPS Incident Lead is responsible for reviewing the IRA; working with the ISM to make any adjustments to the form; and making a final determination about the appropriate risk level (high, medium, or low) and breach/non-breach designation for each incident. In addition, the ISPS Incident Lead will make a final determination about whether or not to invoke the DBMT and, if so, which members to involve, as detailed in the next section.

### 7.5.4 Invoking the DBMT

All incidents require attention, but their risk, characteristics, expected outcomes and the level of effort and resources needed to respond may vary. In performing the above analysis, the ISPS Incident Lead will decide whether to invoke the entire DBMT or a smaller, specialized DBMT; to determine the recommended course of action and manage the incident to closure.

**Full DBMT Participation:** As a general rule of thumb, the ISPS Incident Lead will invoke the DBMT in its entirety in the event of a "significant" data breach or computer security incident. For purposes of this procedure, a significant incident is defined as one that:

- Potentially impacts 100 or more individuals and/or entities; **OR**
- Involves circumstances that are unusual (i.e., no precedent for handling) or that may result in significant reputational damage, cost or media attention; **OR**
- Involves the loss or compromise of critical sensitive information which may significantly affect the FDIC's mission or operations. For help in making this determination, refer to **Appendix A** which provides a link to the current inventory of FDIC critical sensitive information.

**Select DBMT Participation:** For incidents that do not meet the above criteria, the ISPS Incident Lead will convene a smaller, hand-selected DBMT, generally consisting of the Divisional ISM/IR POCs, Legal, CISO, PPM, and/or other appropriate FDIC Program Area Specialists. The ISPS Incident Lead may elect to convene and consult with the DBMT using any channel of communication (i.e., via email, teleconference and/or in-person meetings).

For example, for incidents involving minimum (less than 100) but sensitive information, such as the loss of SSNs, a smaller DBMT should be invoked versusif an incident involves a complex sensitive and PII data loss for multiple stakeholders such as bank customers, a full DBMT should be invoked.

Once it has been determined that a full DBMT should be convened, the ISPS Incident Lead will notify CSIRT and provide periodic status updates thereafter of any key DBMT decisions or actions, as appropriate.

### 7.5.5 Incident Mitigation

Based upon the risk analysis performed in the previous steps, DBMT, will determine and recommend to the CIO/CPO (or designee) an appropriate course of action that includes strategies to mitigate the impact of the incident. The FDIC will make good faith efforts to mitigate any harmful effect that is known to have occurred as a result of a use or disclosure of sensitive information, including BSI and/or PII, in violation of Federal requirements and FDIC's data security/privacy protection policies and procedures. This includes disclosure by the FDIC or its business associates.

The following factors must be considered when determining the need to mitigate any damages:

1. Whether any damage occurred;
2. The nature of the damage that occurred;
3. The amount of damage;
4. The type of data that was used or disclosed;
5. The reasons for the disclosure; and
6. Whether the harm can be mitigated.

Below are examples of possible mitigation methods (this list is not intended to be exhaustive.):

- Notification to affected individuals and entities (see Section 7.6 for external notification guidance.);
- Provision of credit monitoring services to affected individuals and entities; and
- Use of FDIC Call Center to assist affected individuals and businesses (see **Appendix I** for guidance regarding the use of FDIC Call Center.).

## *7.6 External Notification*

This section provides details for matters to be considered in an external notification process.

### 7.6.1 Authorization for External Notification

Authorization by the Executive Office and CIO/CPO is required prior to issuing or conducting external communications or notifications regarding potential or known data breaches, as explained below:

- **FDIC Personnel Disclosures about Incidents** – Unless authorized, FDIC personnel are prohibited from disclosing or causing to be disclosed any information pertaining to an open or closed data breach/incident to any individual who does not have an authorized "need to know" the information.
- **Public Inquiries about Incidents** – In regard to media-related inquires about FDIC data incidents or data breaches, the FDIC Office of Communications (OCOM) serves as the initial point of contact. For non-media-related inquires, the Chief Information Officer Organization (CIOO) will determine who will handle the inquiry.
- **Internal Communication Process for External Notification** – The DBMT will determine the need for external communication and breach notification, in accord with the guidance outlined in the **Appendix K**. The CIO/CPO or authorized designee must approve the recommended course of action and notify the Executive Office prior to the release of external communications or

notification. Additionally, the content of the notification must be approved by Legal, the affected Division/Office, and the CIO/CPO or designee prior to release.

- **US-CERT Reporting** – The requirements noted in the above bullet regarding authorization from senior management prior to external notification do NOT pertain or apply to US-CERT reporting/notification. FDIC CSIRT is required to notify US-CERT within the OMB-mandated one-hour timeframe for PII incidents. For non-PII incidents, CSIRT must report to US-CERT within the required timeframes established by US-CERT (refer to the US-CERT "Federal Incident Reporting Guidelines").

## 7.6.2 External Notification Considerations

Once the DBMT has determined the need for external notification, the following questions must be considered to ensure the appropriate content, timing, method, and recipients of the notification:

### 7.6.2.1 When to start the notification process?

Before issuing external notification, FDIC must first determine the scope of the incident and, if applicable, restore the reasonable integrity of the compromised system or data. The goal is to provide notification to affected individuals/entities without unreasonable delay (generally within 10 days from the date that the analysis of the breach is completed), so that affected individuals and entities can take protective steps quickly. However, notification should not be issued prematurely, based on incomplete facts, or in a manner that compounds harm. In addition, the timing of the notification must be appropriate and consistent with the needs of law enforcement, national security (if applicable), and any measures necessary for the Corporation to determine the scope of the breach and to contain the incident. Thus, in some instances, it may be necessary and appropriate to delay notification. The decision to delay notification will be made by the CIO/CPO or designee and/or the Executive Risk Committee (ERC), after weighing the impact on affected individuals and parties, internal operations, and other relevant stakeholders or entities. Depending upon the type of incident (e.g. PII), notification could involve multiple stakeholders or entities including banks, government agencies (e.g. FFIEC), vendors, service providers, law enforcement, the Executive Branch, Congress, and possibly state and federal regulatory agencies.

### 7.6.2.2 Who will draft and issue the notification?

For the majority of FDIC data breaches, the DBMT will determine and specify who is responsible for coordinating the drafting and issuance of the notification. In general, FDIC Legal is responsible for drafting the notification language or talking points, in coordination with ISPS and the Divisional ISM (or designated subject matter expert). The notice is typically issued by the Head/Director of the affected Division or Office. However, depending on the type of data that was lost, the notice may be issued jointly by the CIO/CPO and the Head of the affected Division/Office.

Depending on the circumstances, a third party such as a financial institution or a vendor may offer to draft and issue the notification. In this instance, the Divisional ISM (or designated subject matter expert) will coordinate this effort with FDIC Legal and ISPS, and notifications may be drafted jointly by a third party.

See sample scenarios below:

**Scenario 1 (FDIC/Financial institution)**: An incident involves the loss, theft or disclosure of sensitive customer information (BSI and/or PII) belonging to an open financial institution. As instructed by the DBMT, those individuals closest with the institution will assist in coordinating corrective actions, including acting as a liaison between FDIC Legal and the affected institution, ensuring that the institution and FDIC Legal are both onboard with the notification language and in agreement on who will send out the notification to affected individuals/entities.

**Scenario 2: (FDIC/Vendor)**: An incident involves the loss, theft or disclosure of sensitive customer information (BSI and/or PII) belonging to FDIC by an outsourced provider (vendor). As instructed by the DBMT, a designated FDIC subject matter expert (SME) will assist in coordinating corrective actions, including acting as a liaison between FDIC Legal, the outsourced provider/vendor, ASB/Contracting Officer and the Divisional Oversight Manager, as well as ensuring that the outsourced provider/vendor and FDIC Legal are both on board with the notification language and in agreement on who will send the notification out to affected individuals/entities.

### 7.6.2.3 What should be included in the notification?

Notifications to affected parties are situational dependent and do not always include remediation assistance such as an offer of credit monitoring services.

The contents of the notification must be concise and in plain language and should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of information involved in the breach (e.g., Report of Examination; watch lists; loan files with personal information such as full name, Social Security Number, date of birth, home address, account number, disability code, etc.);
- A statement about whether the information was protected[18], when it is determined that providing such information would be beneficial and would not compromise the security of the system;
- Suggested steps individuals or parties should take to protect themselves from potential harm, if any;
- A brief description of what the FDIC is doing to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Contact information (toll-free telephone number, e-mail address, postal address).

The content of the notification must be approved by the General Counsel (or designee), the affected Division/Office, and the CIO/CPO (or designee) prior to release.

**Appendix J** presents several notification letter samples.

### 7.6.2.3 How should the notification be provided?

The means for providing notification should be commensurate with the number of individuals/entities affected, what contact information is available about the affected parties and the urgency with which they need to receive notice.

The following means can be considered:

[18] Note: Notification is not necessary if the data was sufficiently protected through encryption.

- **Telephone**: Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals or parties are affected. Telephone notification, however, will be contemporaneous with written notification by first-class mail.
- **First-Class Mail**: First-class mail notification to the last known mailing address of the individual or parties in the Corporation's records will be the primary means by which notification is provided. Where there is reason to believe the address is no longer current, reasonable step(s) will be taken to update the address by consulting with other agencies such as the US Postal Service. The notice will be sent separately from any other mailing so that it is conspicuous to the recipient.
- **E-mail**: Notification by e-mail may be appropriate when an individual or party has provided an e-mail address and has expressly given consent to e-mail as the primary means of communication with the Corporation; the notification is for less than 100 affected; and when customers of a financial institution now in receivership have given express consent for the financial information to contact them by email, and no known mailing address is available. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and www.USA.gov web sites, where the notice may be 'layered' so the most important summary facts are up front with additional information provided under link headings.
- **Existing Government Wide Services**: The FDIC may consider use of Government wide services to provide support services needed, such as USA Services, including the toll free number of 1-800-FedInfo and www.USA.gov.
- **Newspapers or other Public Media Outlets**: Individual notification may be supplemented with placing notifications in newspaper or other public media outlets. The FDIC Call Center can be utilized in handling inquiries from the affected individuals and the public. (See **Appendix I** for guidance regarding the use of FDIC Call Center.)
- **Substitute Notice**: In those instances where the Corporation does not have sufficient contact information to provide notification, substitute notice should be used. A substitute notice consists of a conspicuous posting of the notice on the public homepage of the Corporation (www.FDIC.gov) and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media will include the FDIC Call Center toll-free number where an individual can learn whether or not her/his personal information is included in the breach.
- **Accommodations**: Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 will be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the Corporation webpage.

### 7.6.2.4 Who receives notification?

The DBMT will determine who will receive the notification, whether or not the notice goes to affected individuals/entities, the public media, and/or other third parties affected by the breach.

After convening the DBMT, but prior to incident closure, the ISPS Incident Lead will provide periodic status updates to CSIRT, as applicable and appropriate.

## 7.7 Incident Closure

Closure of an incident will occur after the completion of the investigation, the issuance of external notification (if appropriate), and implementation of suitable mitigation measures. The following actions will be taken to close out an incident or breach that involves BSI and/or PII (excluding those incidents that CSIRT closes upon containment, such as open shares or encrypted laptops or devices where there is a low or non-existent risk of harm):

(b)(2),(b)(5)

[redacted]

### 7.7.1 Records Retention

In accordance with the Federal Records Act, activities documenting the Corporation's investigation and response activities are considered Agency records. The responsible Division/Office, ISM, Privacy and Security officials, FDIC Call Center, CSIRT, and others involved in breach response activities must maintain records of their actions in accordance with FDIC's records retention policies.

[19] Note: Incidents requiring computer forensics to answer legal questions may delay official closure for weeks or months.

## 7.8 After Action Review (AAR) & Lessons Learned

Upon closure of the incident with CSIRT, the final step in the incident response process is for the ISPS Incident Lead to coordinate an assessment of the "lessons learned" and to consider whether modifications to the incident handling procedures are needed. The purpose of conducting a "lessons learned" assessment is to continuously improve the incident handling process and prepare for future incidents, as well as to enhance and strengthen existing protections over information systems and data.

As required, a "lessons learned" meeting* or teleconference* will be held with all applicable parties after a major incident, and optionally after lesser incidents, resources permitting. Multiple incidents can be covered in a single "lessons learned" meeting. The meeting will be held as soon as practical, generally within several days of the closure of the incident. (*In lieu of holding a meeting or teleconference, an email or survey may be distributed to key stakeholders involved in the incident response process, soliciting their input on "lessons learned.") The meeting (or survey) will review what occurred, what was done to respond to the incident, and how well the response effort worked.

Questions[20] to be addressed in the "lessons learned" meeting (or survey) include:

- Exactly what happened, and at what times?
- What was the root cause(s) of the incident?
- How well did staff and management handle the incident?
- Were the documented procedures followed? Do adjustments or changes need to be made to the documented procedures based on this incident?
- What information was needed sooner?
- Were any steps or actions taken that impeded or delayed the response effort? Were any steps or actions taken that improved the overall response effort?
- What could staff and management do differently the next time a similar incident occurs?
- How could information sharing internally or externally with other individuals and organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?

### 7.8.1 Metrics

Effective risk management metrics provide a frame-of-reference for gauging and benchmarking the overall efficiency and effectiveness of the FDIC's breach prevention and response capabilities, while consequently driving operational improvement and enhancing data safeguards. Following are key categories of qualitative and quantitative metrics that FDIC uses to benchmark, tailor, and continuously improve its data breach prevention and response capabilities:

- Reporting and response timelines and compliance (i.e., when was the breach reported to CSIRT, US-CERT, internal and external resources, and affected individuals/ entities)
- Operational and administrative (policy/procedural) compliance and effectiveness (i.e., how many and which specific policies and procedures were violated)
- Program area/regional incident compliance and variance (i.e., which Division/Office is responsible and geographic location of user)
- Asset/data types, attributes and risk

[20] These "lesson learned" questions are based on NIST SP 800-61, *Computer Security Incident Handling Guide.*

- Action categories, types and paths, as applicable (i.e., medium/method in which the breach was perpetrated)
- Agent types, frequency and variances (i.e., internal party/external party/partner who perpetrated or was responsible for the breach)
- Number of breached records and affected individuals/entities
- Cost efficiency (e.g., cost of containment, response efforts, credit monitoring, etc.)

Page 114 of 157

(b)(2),(b)(5)

# 8 LEGAL AND DISCIPLINARY PROVISIONS

This section addresses several legal and disciplinary provisions pertaining to the reporting and disclosure of incidents involving sensitive information, including BSI and PII.

## *8.1 Whistleblower Protection Rights*

(b)(2),(b)(5) In accordance with [redacted] the FDIC protects the rights of all current and former employees and applicants for employment at the Corporation from retaliatory action or reprisal for whistleblowing.

## *8.2 Types of Disclosures: Incidental, Accidental, and Intentional*

### i. Incidental Disclosures

Incidental disclosures of SI (BSI and PII) occur as a result of the normal course of business, and which are incidental to an otherwise permitted use or disclosure of the information.

a. If a member of the workforce is taking reasonable precautions, and another individual happens to see or overhear SI that the workforce member is using, the workforce member will not be held liable for that disclosure.

b. Reasonable precautions include:

   i. Keeping one's voice low while discussing information;

   ii. Moving to as private a location as possible while using information; and

   iii. Keeping SI in paper and electronic formats covered or otherwise inaccessible to those who do not have authorization or a legitimate need to know the information.

c. Incidental disclosures are not considered privacy/security incidents and do not usually need to be reported. However, members of the workforce should use professional judgment in assessing the potential outcome(s) of an incidental disclosure and report any disclosures that may result in a fraudulent or criminal misuse of the information or have a negative impact on the FDIC.

### ii. Accidental Disclosures

These are the unintentional disclosures of SI (BSI and PII) that occur as a result of carelessness and/or failure to follow established policies and procedures but are without malicious or premeditated intent.

a. All members of the workforce are required to acknowledge and report known and suspected accidental disclosures of BSI and PII immediately so that:

   i. The situation can be investigated; and

   ii. Damage can be minimized or averted.

b. Accidental disclosures are considered incidents and must be reported immediately to the CSIRT (via the FDIC Help Desk) and the Supervisor or Oversight Manager. Examples of accidental disclosures include, but are not limited to:

   i. Disclosure of BSI or PII to a person requesting the information without verifying the person's identity and authority first;

ii. Leaving BSI or PII materials unattended in a public area and being unable to retrieve or find them after the fact;

iii. Disposing of intact BSI or PII documents or electronic media in unsecured waste receptacles (e.g. without shredding hardcopy documents or appropriately sanitizing media);

iv. Sending an email message that contains BSI or PII to the wrong person by mistake; and

v. Leaving a message that contains BSI or PII on someone else's answering machine.

c. Members of the workforce should assist in correcting or recovering from a disclosure ONLY if instructed to do so by the ISPS Incident Lead or the DBMT.

### iii. Intentional Disclosures

Disclosures of BSI and/or PII that occur as a result of deliberate and/or pre-meditated disregard of established policies and procedures, with or without malicious intent.

1. All members of the workforce are obligated to report any known and suspected intentional disclosures of BSI or PII immediately. Examples of intentional disclosures include, but are not limited to:

   i. Gaining access to BSI or PII by deliberately circumventing security measures, by using someone else's password, or by other fraudulent means;

   ii. Intentionally disclosing BSI or PII to unauthorized persons; and

   iii. Intentionally disclosing BSI or PII to harm others by, or to personally profit from, the disclosure.

Intentional disclosures are considered breaches and will ordinarily result in disciplinary action and the application of sanctions by the FDIC, and may also result in personal liability, either in civil or criminal legal action.

## *8.3 Compliance and Disciplinary Actions (Rules and Consequences)*

Members of FDIC's workforce who fail to comply with the FDIC's privacy/security policies and procedures or with the requirements of federal privacy/security laws or regulations will be disciplined in accordance with the FDIC's normal disciplinary procedures, up to and including termination of employment. Additionally, outsourced service providers who fail to comply with the information privacy/security requirements stipulated in their contracts and Confidentiality Agreements could face monetary penalties, legal action and/or termination of their contracts.

Based on the outcome of the investigation and consultation with the DBMT for confirmed violations (see **Appendix N**, Definitions), the Division/Office Head in consultation with DOA, Human Resource Branch, and with the CIO/CPO may recommend sanctions and disciplinary or adverse actions in accordance with the Corporation "Rules and Consequences" policy as defined in FDIC Circular 2750.1, *Disciplinary and Adverse Actions*.

a. In deciding what action to take for violations of the Corporation's privacy/security and data protection policies, the following factors, among others, are considered:

   i. The nature of the violation,

   ii. The severity of the violation,

iii. Whether the violation was intentional or unintentional, and

iv. Whether the violation indicates a pattern or practice of improper use or disclosure of BSI and/or PII.

b. Depending on the circumstances and impact of the violation, corrective action may range from a verbal warning to separation from employment or removal from/ termination of the contract (if applicable).

c. All privacy and security-related sanctions that are applied by the FDIC will be documented in the employee's personnel file.

# APPENDIX A: CRITICAL AGENCY SENSITIVE INFORMATION INVENTORY

The current inventory of critical agency/business sensitive information is available at:

(b)(2),(b)(5)

[redacted]

# APPENDIX B: EXAMPLES OF REPORTABLE INCIDENTS

The table below provides descriptions and specific examples of incidents – including both potential and actual data breaches – that should be reported immediately upon discovery or detection.

| **Examples of Reportable Data Incidents**<br>***This list is not intended to be exhaustive.*** | | |
|---|---|---|
| **Medium / Manner** | **Description** | **Examples** |
| **External / Removable Media**<br>*Examples:*<br>• *Flash Drive*<br>• *Hard Drive*<br>• *CD/CD-ROM* | A lost or stolen device that contains BSI and/or PII; or an attack executed from removable media (e.g., flash drive/thumb drive, CD) or a peripheral device that compromises BSI and/or PII. | An employee loses a flash drive containing bank examination data. |
| **Verbal Conversations / Disclosures**<br>*Examples:*<br>• *Telephone Conversations*<br>• *In-Person Conversations or Meetings*<br>• *Voicemail Messages* | An indiscrete conversation that discloses BSI and/or PII to individuals who are not authorized to know the information, whether intentionally or unintentionally. | An employee tells unauthorized persons about an upcoming bank closing.<br>An employee mistakenly leaves a voice message containing sensitive information about a terminated employee with an individual not authorized to know that information. |
| **Hardcopy / Physical Records**<br>*Examples:*<br>• *Hardcopy Documents*<br>• *Boxes*<br>• *Faxes*<br>• *Print/Copy Jobs*<br>• *Packages*<br>• *Mail Shipments* | A lost or stolen physical record containing BSI and/or PII; or the unauthorized disclosure or acquisition of a hardcopy record containing BSI and/or PII. | An employee disposes of boxes containing sensitive information in a dumpster.<br>A supervisor discovers that a paper file containing employee SSNs and evaluations is missing from her desk.<br>A sensitive bank examination report is mistakenly faxed by an FDIC employee to a third-party vendor that is not authorized to receive the information.<br>A package of paper files and CD-ROMs containing sensitive depositor data is lost during shipment. |
| **Electronic Equipment**<br>*Examples:*<br>• *Laptop*<br>• *Desktop*<br>• *Blackberry*<br>• *Smartphone* | The loss or theft of a computing device or media used by FDIC personnel, such as a Blackberry, laptop or smartphone, on which BSI and/or PII is stored. | An employee discovers her laptop used to conduct bank examinations has been stolen or lost. |
| **Email**<br>*Examples:*<br>• *Unencrypted email*<br>• *Phishing email* | An email message or attachment containing BSI and/or PII that is sent unsecured/unencrypted; or that is sent to a recipient who is not authorized to view/access the data in the message; or an attack executed via an email message or attachment that compromises BSI | An employee sends an unencrypted email with sensitive claims data to a non-FDIC account.<br>An employee mistakenly sends an unencrypted email with sensitive background investigation data to the wrong recipients. |

| | | |
|---|---|---|
| | and/or PII. | |
| **Improper Usage/Policy Violation**<br>*Examples:*<br>- *Open Shares*<br>- *FTP Traffic*<br>- *Access* | Any incident involving BSI and/or PII that results from a violation of the FDIC's privacy, security, or acceptable usage policies. | An employee misused administrator privileges to gain unauthorized access to a database containing government credit card numbers and PINs.<br>An open share is discovered, potentially making available 2,000 confidential bank examination documents. |
| **Servers & Systems** | Unauthorized access to BSI and/or PII stored in a system, whether intentional or unintentional; or an attack that compromises the confidentiality of BSI and/or PII stored in a system. | A system is hacked into, potentially making available sensitive personnel files of FDIC employees.<br>An employee inadvertently acquires access to seven other employees' performance ratings in an HR database.<br>A keylogger program is installed on an employee's laptop, allowing the capture of login and password information.<br>A remote access tool that is communicating with an external host is found on server/laptop/desktop.<br>A compromised host is discovered on an employee's desktop that has unencrypted sensitive financial data. |
| **Web** | The posting of BSI and/or PII to an unsecured website or public website; or an attack executed to a website or web-based application that compromises BSI and/or PII. | A glitch on the Corporation's internet webpage allows unauthorized read-only access to a database containing sensitive bidder information.<br>A document containing CAMEL ratings for all open banks is posted on the FDIC's intranet page. |

# APPENDIX C: INCIDENT PREVENTION/PREPARATION SUPPLEMENTAL GUIDANCE

## Corporate Strategies for Preventing Data Breaches

The first step in the incident response process is taking appropriate actions to prepare for and prevent a data breach from occurring. The FDIC implements a variety of administrative, technological and physical measures to help reduce the risk of a data breach occurring, including *but not limited* to:

- Establishment and training of a Computer Security Incident Response Team (CSIRT) whose duties and responsibilities are detailed in the **Roles and Responsibilities Section** of this manual
- Security protection engineering and data loss prevention (DLP) capabilities; data encryption and network/system/host security controls; virus and malware protection; and continuous monitoring of FDIC systems/applications;
- Periodic privacy/security compliance and risk assessments of FDIC offices, programs, and outsourced vendors;
- Physical security controls such as shredders, locks, guards, badges, and other methods of physical identification;
- Comprehensive policies and procedures centered on data privacy, security, and breach prevention. Additional administrative measures include the development and enforcement of rules and consequences policies for employees and contractors involved in incident reporting and handling;
- Risk management metrics and incorporation of lessons learned from past incidents into agency security and privacy policies and practices; and
- Targeted awareness and training to educate users and incident response participants about their roles and responsibilities for preventing, reporting and responding to known and suspected data breaches.
    - As a first step in the training process, all FDIC employees and contractors must complete mandatory Corporate Information Security and Privacy Awareness training on an annual basis, which requires them to affirm their understanding of their responsibilities for safeguarding agency-sensitive information and personally identifiable information and for immediately reporting the loss, theft or compromise of such data to the FDIC Help Desk/CSIRT and their immediate Supervisor or Oversight Manager. Employees with significant responsibilities for information security must complete specialized training on their IT security responsibilities and established system rules, prior to being granted access to IT applications and systems. Specialized divisional training is also required for employees prior to granting access to major applications.
    - In addition, targeted, role-based training is available for the DBMT, ISPS Incident Lead, Divisional ISMs, Supervisors/Oversight Managers, and others involved in the incident response process. The FDIC also designs and runs periodic data breach simulations (tabletop exercises / fire drills) that drive awareness, support incident response team training, and help identify gaps to continuously improve the FDIC's incident response capabilities and preparedness. On a biennial basis, the FDIC Privacy Program conducts privacy clinics which provide targeted training to FDIC employees on data breach prevention. Contact the FDIC Privacy Program at privacy@fdic.gov for more information.

## Steps You Can Take to Prevent a Breach

FDIC employees and contractors are responsible for protecting all FDIC-provided data, in both hardcopy and electronic format. For practical tips and steps you can take to prevent a data breach, refer to the *Preventing Data Breaches at FDIC Presentation* available on FDIC's internal Privacy Program webpage at:

(b)(2),(b)(5) [redacted]

# APPENDIX D: 'INFOALERT' DISTRIBUTION LIST

- Chief Information Officer (CIO)/Chief Privacy Officer (CPO)
- Division of Information Technology (DIT) Director
- Deputy to the Chairman for Communications
- Office of Communications (OCOM) Assistant Director
- Chief Information Security Officer (CISO)
- Security Protection Engineering Section (SPES) Chief
- Security and Policy Compliance Section Chief
- Privacy Program Manager (PPM)
- Legal Division Assistant General Counsel and Designated Legal Counsel
- (b)(2),(b)(5) [redacted]
- (b)(2),(b)(5) [redacted]

# APPENDIX E: DIVISIONAL INCIDENT RESPONSE (IR) POCS

The current listing of Divisional IR POCs is available at:

(b)(2),(b)(5) [redacted]

# APPENDIX F: DIVISION INCIDENT RESPONSE GUIDELINES

FDIC Divisions/Offices have published supplemental guidelines to assist their staff and contractors with reporting and responding to data incidents. These divisional guidelines feed into the Corporate-wide data breach response procedures outlined in this guide. Links to the various Division/Office incident response guidelines are provided below.

(b)(2),(b)(5)

| Division/Office | Link to Divisional IR Guidelines |
|---|---|
| Division of Finance (DOF) | [redacted] |
| Division of Depositor and Consumer Protection (DCP) | [redacted] |
| Division of Resolutions and Receiverships (DRR) | [redacted] |
| Division of Risk Management Supervision (RMS) | [redacted] |

(b)(2),(b)(5)

Page 125

Page 126 of 157

(b)(2),(b)(5)

Page 126

Page 127 of 157

(b)(2),(b)(5)

Page 128 of 157

(b)(2),(b)(5)

Page 129 of 157

(b)(2),(b)(5)

Page 129

Page 130 of 157

(b)(2),(b)(5)

(b)(2),(b)(5)

Page 132 of 157

(b)(2),(b)(5)

(Please review page 3 of the notification letter.)

[Back to top]

### 11. Can this happen again?

The FDIC regrets that this possible disclosure has occurred as a result of its contractor not following standard procedures adopted by the FDIC for the physical transmission of sensitive data. The contractor has now adopted the standard FDIC procedures for the transmission of sensitive data. Additionally, the FDIC will continue our investigation in an effort to locate and secure the missing electronic storage device.

(Please review page 1 and 2 of the notification letter.)

[Back to top]

### 12. How do I update my contact information with you?

In order to update your contact information, I can take the information over the phone at this time.

[Back to top]

### 13. I represent a TV/Newspaper/Radio and would like some information.

**Contact:**

**David Barr**
**Office: (202) 898-6992**
**E-mail: dbarr@fdic.gov**

[Back to top]

### 14. What is the contact information for the three credit reporting agencies?

**Equifax:**
PO BOX 740241
Atlanta, GA 30374
Or call: 1-800-525-6285
Online at: www.equifax.com

**Experian:**
PO BOX 2002
Allen, TX 75013
Or call: 1-888-397-3742
Online at: www.experian.com

**TransUnion:**
PO BOX 6790
Fullerton, CA 92834
Or call: 1-800-680-7289
Online at: www.transunion.com

(Please review page 3 of the notification letter.)

[Back to top]

**15. I have not received a letter – am I on the list?**

You may be an individual for whom we had no mailing address. Let me take your name and contract information; we will review our records and someone will be in contact with you within 3-5 business days.

[Back to top]

**16. I received the notification on behalf of a deceased relative; what should I do?**

Upon the death of a consumer, the three major credit reporting agencies, Equifax, Experian and Trans Union, will flag the deceased person's credit file. This will prevent the deceased's credit file information from being used to open credit in the event that someone tries to steal their identity. The process is to mail a copy of the death certificate to each company listed on page 3 of the notification letter.

Upon receipt of the death certificate, the credit reporting agencies will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, the credit agency will place a seven year promotional block on the deceased consumer's file. Once the credit reporting agency has completed their research, they will send a response back to the spouse, attorney, or executor of the estate.

[Back to top]

**17. When I called Experian, they asked for my Social Security Number. Is it okay to give it to them?**

Yes. The credit reporting agencies ask for your Social Security Number and other personal information in order to identify you and avoid sending your credit report to the wrong person. It is okay to give this information to the credit reporting agency that you call. However, you should be vigilant on releasing your personally identifiable information to any third party.

[Back to top]

**18. How do I know that this is not a scam?**

You can find Experian online at: www.experian.com or you can validate the Internet site for yourself by using one of the commonly available Internet search engines, or you can contact them directly at 1-888-397-3742. Once you have contacted Experian, you will be able to obtain credit monitoring services free of charge for two years.

(Please review page 3 and 4 of the notification letter.)

[Back to top]

# APPENDIX J: SAMPLE WRITTEN NOTIFICATION

## *Sample Letter 1*

This is an example of a letter where credit monitoring is recommended, but not provided, to individuals.

[*Date*]

Dear [*Insert name*]:

Recently we were advised of a possible security breach involving [*explain the kind of personally identifiable information or sensitive data that was involved*]. [*If possible, briefly detail incident that led to possible breach. Include when the breach occurred or was discovered*]. The Corporation regrets that this release of personal information occurred and is taking steps to mitigate the possibility of such a breach occurring in the future.

Our purpose in notifying you is to ensure that you are aware of the steps you can take to protect yourself from any further use of this information. We urge you to contact the three major credit bureaus to ascertain whether your credit has been affected and to alert them to the fraudulent use of your identity. We suggest that you obtain a full credit report from the credit bureaus and review the reports closely for any suspicious activity. Recent federal legislation grants all consumers the ability to obtain annually a credit report, free of charge, from each of these three credit reporting agencies (listed below). We urge you to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the police and the credit bureaus.

We also recommend that you place a fraud alert on your credit report. Individuals can place a fraud alert on their consumer reports for 90-days, for free. When you place these alerts, anyone accessing your credit report in the next 90 days will receive the fraud flag with the report and by law, they have to take extra steps to identify the person that is seeking credit. If identity thieves are seeking credit, this alert will help prevent them from opening fraudulent credit in your name. Providing a police report to the credit bureaus will keep this alert on their records beyond the 90 day period.

The process of placing a fraud alert is entirely automated, and takes about two minutes. If you call one credit bureau and provide correct identifiers (social security number, the number portion of your home address, and two digit year of birth), they will process the alert and forward it on to the other two nationwide consumer reporting agencies.

To place a fraud alert, call the fraud departments of any of these credit reporting agencies: Equifax at 800-525-6285, Experian at (888) 397-3742, and TransUnion at (800) 680-7289. Get addresses and other details at www.equifax.com, www.experian.com and www.transunion.com.

For additional information on identity theft, you may visit the Federal Trade Commission (FTC) website at www.ftc.gov/bcp/edu/microsites/idtheft or write FTC, Consumer Response Center, Room H-130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

We will continue to monitor this situation and will provide further information as it becomes available. Questions regarding this notification can be sent to [*contact information including any names, telephone numbers, postal addresses, e-mail addresses, or website links*]. [*If needed, provide contact information for the law enforcement agency that is investigating the incident*]

Sincerely,

[*Name*]

[*Title*]

## *Sample Letter 2*

This is an example of a letter where credit monitoring is provided to individuals.

[*Date*]

Dear [*Insert Name*]:

We were recently advised of a possible security breach involving [*explain the kind of personally identifiable information or sensitive data that was involved*]. [*If possible, briefly detail incident that led to possible breach. Include when the breach occurred or was discovered*]. The FDIC regrets that the breach occurred and is taking steps to mitigate the possibility of such a breach occurring in the future.

We are contacting you to let you know what the FDIC is doing to protect you and to ensure that you are aware of the steps you can take to protect yourself from possible misuse of this information, including contacting the three major credit bureaus to obtain a free, full credit report and reviewing each of them closely for any suspicious activity. Federal legislation grants all consumers the ability to obtain annually a credit report, free of charge, from each of the three credit reporting agencies. The three agencies have set up a central website and toll-free telephone number. These are available at www.annualcreditreport.com or by phone at 1-877-322-8228.

FDIC is providing you a two-year credit monitoring service called "Triple Advantage®" from ConsumerInfo.com, Inc. an Experian® company. This service also includes assistance with identity theft protection including identity theft insurance. **The FDIC is making this service available to you at no cost.** Enrolling in this program will not hurt your credit score.

To enroll in Experian's credit monitoring program, visit the website listed below and enter your individual activation code as provided below. If you prefer, you can enroll with Experian over the phone by calling 1-866-252-0121.

**Experian Triple Advantage Web Site: http://partner.experiandirect.com/premium**
**Your Experian Activation Code: [Activation Code]**
**You Must Enroll By: [Enrollment Deadline Date]**

As soon as you enroll in the Triple Advantage program, Experian will begin to monitor your credit reports from Experian, Equifax® and TransUnion® on a daily basis and notify you of key changes. This tool will help you identify potentially fraudulent use of your information, and provide you with immediate assistance from a dedicated team of fraud resolution representatives should you ever need help.

Triple Advantage membership includes:

- A free copy of your Experian, Equifax and TransUnion credit reports.
- Daily monitoring and alerts of changes to your credit reports—to include activity you should be aware of such as notification of new inquiries, newly opened accounts, delinquencies, public records or address changes.
- Access, as needed, to your Experian credit report and PlusScore℠ for the duration of your membership.
- Toll-free access to Experian's fraud resolution representatives who will help you investigate each incident; contact credit grantors to dispute charges, close accounts if need be, and compile documents; and contact all relevant government agencies.
- $25,000 in identity theft insurance coverage provided by American International Group, Inc. for certain identity theft expenses[21].

[21] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**You can activate your membership by visiting**
**http://partner.experiandirect.com/premium.**
**Or call 1-866-252-0121 to register with the activation code above.**

Once your enrollment in Triple Advantage is complete, you should carefully review your credit reports for inaccurate or suspicious items. If you have questions about Triple Advantage, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care at 1-866-252-0121.

If you choose not to enroll in the Experian program, for any reason, we suggest that you contact the three major credit bureaus to obtain a free, full credit report and review each of them closely for any suspicious activity. Federal legislation grants all consumers the ability to obtain annually a credit report, free of charge, from each of the three credit reporting agencies shown below. The three agencies have also set up a central website – www.annualcreditreport.com – and central toll-free telephone number – 1-877-322-8228.

Equifax:
P.O. Box 740241
Atlanta, GA 30374
Or call:
1-877-478-7625
Online at:
www.equifax.com

Experian:
P.O. Box 2002
Allen, TX 75013
Or call:
1-888-397-3742
Online at:
www.experian.com

TransUnion:
P.O. Box 6790
Fullerton, CA 92834
Or call:
1-800-680-7289
Online at:
www.transunion.com

Fraud Alert

A fraud alert is an option that is available at no additional cost. A fraud alert is a consumer statement added to your credit report that alerts creditors that you may be a fraud victim and requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. We encourage you to review your account statements carefully and report any suspicious activity to the institution issuing them. We also recommend that you periodically review your credit reports, and if you discover information related to any fraudulent activity, ask that the information be deleted. You should also report suspicious activity to your local police or sheriff's office and file a report of identity theft.

For additional information on identity theft, you may visit the Federal Trade Commission (FTC) website at www.ftc.gov/bcp/edu/microsites/idtheft or write FTC, Consumer Response Center, Room H-130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

We will continue to monitor this situation and will provide further information as necessary. If you have any questions, need any information, or require any assistance in regard to this matter, you may contact the FDIC at [*contact information including any telephone numbers, postal addresses, e-mail addresses, or website links*].

Sincerely,

[*Name*]

[*Title*]

## *Sample Letter 3*

This is an example of a letter where credit monitoring is provided to a commercial entity.

[*Date*]

Dear [*Insert Name*]:

We were recently advised of a possible security breach involving [*explain the kind of sensitive information that was involved*]. [*If possible, briefly detail incident that led to possible breach. Include when the breach occurred or was discovered*]. The FDIC regrets that the breach occurred and is taking steps to mitigate the possibility of such a breach occurring in the future.

We conducted a thorough review of the situation and determined that you were among the small number of commercial customers whose information was compromised. We have no reason to assume that the information was specifically targeted or was misused, and we also have no reason to believe your organization's finances are at risk. Nonetheless, the fact that the theft occurred means that certain precautions are desirable. Consequently, the FDIC has arranged to have a business credit monitoring service made available to you for 24 months at no cost to you, which includes unlimited access to your business credit report. This service is part of Experian and is known as the Business Credit Advantage$^{SM}$. The Experian Business Credit Advantage service includes:

- Monitoring of your business credit file with Experian
- Unlimited access to your Experian's business credit report
- Email alerts of key changes indicating possible fraudulent activity

You have until January 31, 2014 to activate this membership, which will then continue for 24 full months. We encourage you to activate your business credit monitoring membership quickly.

To sign up online, please visit the Web site from the link below and follow the instructions. You will be asked to enter your Activation Code and search Experian's database for your business. All business credit reports will be accessible to you online and alerts will be delivered via email to the email address you register.

-Your Business Credit Advantage Activation Code: **[insert Activation code]**
-Web site to redeem code: **http://www.SmartBusinessReports.com/ProtectMyCompany**
-Experian phone number for assistance redeeming your code online: **(800) 303-1640**

If you choose not to enroll in the Experian program, for any reason, we suggest checking your business records regularly, signing up for email alerts, monitoring credit reports on a regular basis, and reporting any irregularities or problems immediately to the appropriate credit monitoring agency or to the appropriate Secretary of State's office.

We have also provided contact information for the three major credit reporting agencies.

| TransUnion: | Experian: | Equifax: |
|---|---|---|
| 1-866-922-2100 | 1-800-520-1221 | customerservice@equifaxsmallbusiness.com |
| Online at: | Online at: | Online at: |
| www.transunion.com | www.experian.com | www.equifax.com |

FDIC takes the confidentiality and protection of your account information very seriously. The FDIC regrets any inconvenience this may cause you, and is taking steps to mitigate the possibility of such a breach occurring in the future. We will continue to monitor this situation and will provide further information as necessary. Please feel free to contact me at [Insert Telephone Number] with any questions you may have.

Once again, we apologize for any inconvenience which may result from this theft of information.

Sincerely,

[*Name*]

[*Title*]

# APPENDIX K: INCIDENT RISK ASSESSMENT GUIDELINES

In order to assess the potential impact of a breach and determine the appropriate course of action, the ISPS Incident Lead, in coordination with the Divisional ISM/IR POC(s), will perform an incident risk assessment, using the following five (5)-factor risk assessment methodology as a guide. The Data Breach Management Team (DBMT) will review this analysis and determine an appropriate course of action to mitigate harm posed by the breach, including whether external breach notification and communications are warranted.

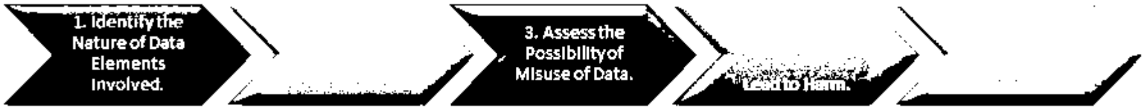

1. Identify the Nature of Data Elements Involved.
3. Assess the Possibility of Misuse of Data.
Lead to Harm.

*Figure 1. Five (5) Factor Incident Analysis Methodology*

Each of the above steps is detailed in the subsections below. Balanced collectively, these five steps will help determine the necessity of notification, the speed of notification, and the necessity of remuneration in the event of a breach of SI, including BSI and/or PII.

The above 5-factor methodology is based on Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and Federal Information Processing Standards (FIPS) guidance, which utilize the impact levels of Low, Moderate and High to categorize the potential impact or harm that could result if data were inappropriately accessed, used or disclosed. The table below defines the three (3) impact levels, which can be used to assess the incident, as detailed in the subsections below.

***Table 2.[22] Potential Impact Levels***

| | | |
|---|---|---|
| **Low** | The loss of confidentiality, integrity, or availability is expected to have a **limited adverse effect** on organizational operations, organization assets or individuals. | This means there might be (i) degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) minor damage to organizational assets; (iii) minor financial loss; or (iv) minor harm to individuals. |
| **Moderate** | The loss of confidentiality, integrity, or availability is expected to have a **serious adverse effect** on organizational operations, organization assets or individuals. | This means there might be (i) a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) significant damage to organizational assets; (iii) significant financial loss; or (iv) significant harm to individuals that does not involve loss of life or serious life threatening injuries |
| **High** | The loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic adverse effect** on organizational operations, organization assets or individuals | This means there might be (i) a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) major damage to organizational assets; (iii) major financial loss; or (iv) severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. |

[22] Table 2 is based on Federal Information Processing Standards Publication 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, which defines three levels of *potential impact* on organizations or individuals should there be a breach (i.e., a loss of confidentiality, integrity, or availability).

### *Step 1. Identify the Nature of Data Elements Involved.*

When determining when and how to notify affected individuals and/or entities, the first step is to consider the nature of the data elements involved in the breach. An assessment of the nature of the data elements takes into account three primary factors, as illustrated in the figure below:

A. The specific type and elements of data that were lost, stolen, or otherwise compromised;
B. The "context of use" of the data (i.e., how the data is used or combined with other data); and
C. The sensitivity level of the data.

*Figure 3. Nature of Data Elements*

Some data is sensitive as a stand-alone element, such as Social Security Number (SSN), Taxpayer Identification Number (TIN), or a CAMEL rating. However, some data can become sensitive based on its "context of use," which refers to how the data is used or combined with other data. For example, a name is generally considered non-sensitive PII. However, a name can become sensitive in combination with certain data (e.g., an individual's name + birth date + mother's maiden name; or a commercial entity's name + financial account number + account balance). Additionally, some data can become more sensitive based on its context. For example, a list of the names of employees who signed up for an informational newsletter is generally considered non-sensitive, whereas a list of employees who were terminated for misconduct is considered sensitive. Thus, it is critical to fully understand and balance the "context of use" in order to accurately determine the overall sensitivity level of the data.

After assessing the overall sensitivity of the data, the nature of the data elements can be categorized into one of three levels of risk: Low, Moderate, or High. Table 4 (below) provides examples of how specific agency/ business sensitive and PII data elements may fit within these three categories.

***Table 4. Risk Levels for Nature of Data Elements – Examples***

| **Risk Level** | **Personally Identifiable Information (PII) Examples** | **Agency/Business Sensitive Information (BSI) Examples** |
|---|---|---|
| **Low** | Compromise of an FDIC system containing the full names, job titles, *work* email addresses, and *office* telephone numbers of subscribers to FDIC special media alerts. | Compromise of an FDIC system containing aggregate, statistical data on financial institutions. |
| **Moderate** | Compromise of an FDIC system that contains the full names, job titles, *personal* email addresses, and *home* addresses of individuals who attended an FDIC workshop. | Compromise of an FDIC system containing stockholder listings for commercial entities, including certificate owners, numbers and balances. |
| **High** | Compromise of an FDIC system containing the full names, home addresses, and Social Security Numbers (SSNs) of loan customers of a failed financial institution. | Compromise of an FDIC system containing Failing Bank Board Cases and confidential Supervisory Reports for over 100 financial institutions. Or, compromise of a system containing Tax ID Numbers, Certificate Owners, Certificate Numbers, and |

[redacted] Certificate Balances.

The more sensitive the data involved in the breach, the more likely the DBMT is to recommend that the FDIC release a notice of the breach (assuming there are no mitigating factors, such as data encryption). In cases where the data is determined to have a low sensitivity level, the DBMT may recommend that no notice is necessary.

### *Step 2. Determine the Number of Individuals and/or Entities Affected.*

Another consideration when determining the potential impact of a breach is how many individuals or entities are affected by the breach. Incidents involving 10 million records versus 10 records may have a larger impact, both in terms of the cost of mitigating the incident and the collective harm to affected individuals/entities, the Corporation, and the financial sector, as applicable.

The number of affected individuals/entities may influence the *method* of notification employed by the Corporation, but it is **not a determining factor for whether or not to provide notification.**

This factor also may impact the decision as to who should be involved for purposes of investigation, notification, and mitigation. The ISPS Incident Lead will generally invoke the entire DBMT for incidents that require notification to a large number of individuals/entities (100+) to assist with logistical and substantive issues raised by the incident. Refer to Section 7.5.3 for more information.

### *Step 3. Assess Likelihood Data is Accessible and Useable (Probability of Misuse of Data).*

Once the number of individuals/entities affected by the breach has been determined (Factor 2), the next step is to assess the possibility of misuse. The possibility of misuse refers to the likelihood that the data is accessible or usable by unauthorized individuals. The greater the possibility of misuse for items such as identity theft, the more likely the DBMT is to recommend a quick release of the breach notification.

In assessing the probability of misuse, consideration should be given to whether the data has a Low, Moderate or High risk of being compromised. This assessment should be guided by NIST security standards and guidance, and should take into account several factors, including but not limited to:

- The medium/format in which the data was lost, stolen or compromised (e.g., paper, email, thumb drive, system, web posting, etc.);
- Any associated physical, technological and/or procedural safeguards or controls in place to protect the data (e.g., encryption, password-protection, etc.) and the relative strength/weakness of these controls (e.g., password strength or weakness, NIST-validated encryption method versus a weak or well-known encryption algorithm, etc.); and
- The circumstances of the breach, such as how the breach occurred, whether the data was targeted intentionally, who gained access to it and their intent (if known), the likelihood that any unauthorized individuals will know the value of the information and use the information or sell it to others, etc.

**Even if data has been lost or stolen, this does not necessarily mean that it has been or can be accessed or used, depending upon the controls in place to protect the data. If the data is adequately protected, for example by a NIST-validated encryption method, the actual risk of compromise is low to non-existent.** Likewise, open shares (i.e., improperly configured access controls that are discovered on FDIC's internal network shared folders) are reported and tracked via FDIC's Incident Response process; however the FDIC does not consider the information contained within the associated internal shared folders to be at risk of breach unless evidence to the contrary is provided at the time the access control deficiency is reported.

The table below provides examples of how to categorize the probability of misuse of data.

**Table 6. Probability of Misuse of Data – Examples**

| Risk Level | Personally Identifiable Information (PII) Examples | Agency/Business Sensitive Information (BSI) Examples |
|---|---|---|
| Low | Email was sent that contained the names, addresses and last four digits of SSNs of bank customers. The email was encrypted, but mistakenly sent to the wrong employee who confirmed she deleted the email.<br>Letter containing SF-50 was mistakenly mailed to the wrong FDIC employee. The recipient immediately alerted FDIC and returned the letter and SF-50. | FDIC-issued flash drive was lost that contained stockholder listings for commercial entities. Flash drive was encrypted using NIST-validated encryption method.<br>Open share containing Corporate financial data discovered on FDIC's internal network and immediately locked down. |
| Moderate | Laptop was lost that contained the names, home addresses, and government-issued credit card numbers of employees. Data was password-protected, but a NIST-validated encryption method was <u>not</u> used. | Employee mistakenly posted a stockholder listing containing certificate owners, numbers, balances and TINs for commercial entities. Listing was posted on an external FDIC website, but was discovered by employee and pulled down within 24 hours. |
| High | Examiner's laptop was stolen that contained the names, home addresses, and SSNs. Laptop and data were not encrypted or password protected. | Computer hacker targeted and accessed FDIC system containing Failing Bank Board Cases for over 100 financial institutions. |

## *Step 4. Analyze the Likelihood that the Incident May Lead to Harm.*

When analyzing the likelihood that an incident may lead to harm, the following factors should be weighed:

**A. Broad Reach of Harm** – The loss or compromise of BSI and/or PII can result in a broad range of potential harms not only to affected individuals and entities, but also to the Corporation and the financial institutions it is responsible for examining and supervising. Under the *Privacy Act*[23], agencies must protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." Examples of possible harms to individuals include, but are not limited to:

- Identity theft or fraud[24]
- Financial harm
- Potential for blackmail
- Disclosure of private facts that could cause mental pain and emotional distress
- Disclosure of address information for victims of abuse
- Potential for secondary uses of information which could result in fear or uncertainty
- Exposure of data that could cause humiliation, embarrassment or loss of self-esteem

Examples of possible harms to affected entities and/or FDIC include, but are not limited to:

- Reputational damage to the Corporation and/or affected entities
- Loss of public trust in FDIC operations
- Disruption to and/or loss of confidence in the nation's financial system
- Financial and/or operational damage or costs to the Corporation and/or affected entities

**B. Likelihood of Harm Occurring** – The probability that harm will occur from a breach depends on several factors, namely the circumstances of the incident, the type(s) of data involved, and the "context of use" of the data. For example, certain types of information are useful for perpetrating identity theft, such

[23] 5 U.S.C. § 552a(e)(10).

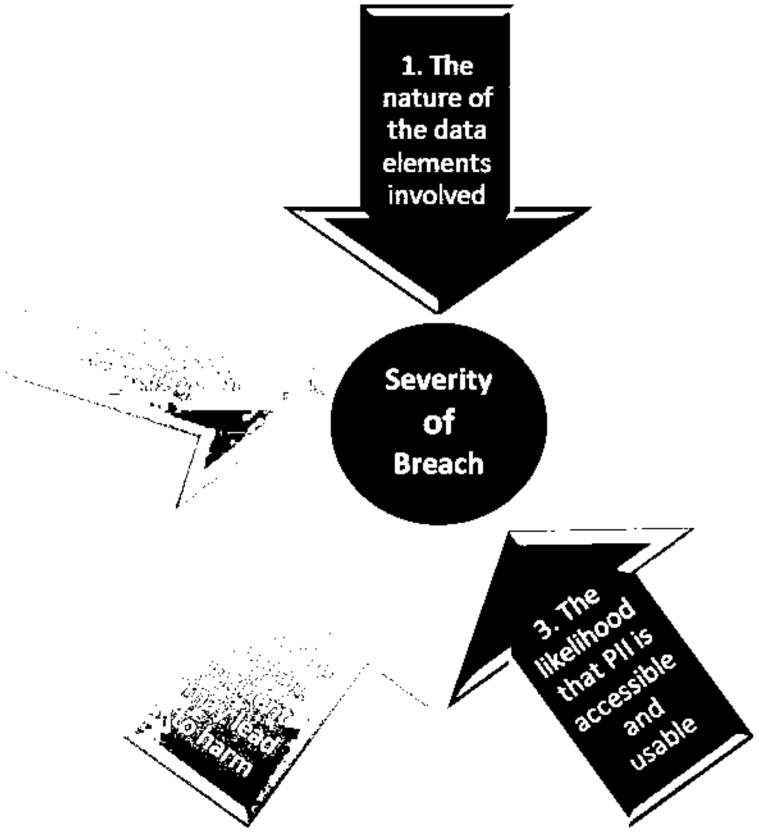
[24] For guidance in considering whether the loss of data could result in identity theft or fraud, the core incident management group should consult the "Recommendations for Identity Theft Related Data Breach Notification" issued by the Identity Theft Task Force, which is available at: www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

as a Social Security Number, account information, date of birth, passwords, mother's maiden name, or other data used to authenticate or verify an individual's identity (e.g., fingerprint, driver's license or state identification number, etc.). However, if the compromised information includes only names and addresses, the likelihood of identity theft occurring may be low to non-existent. Conversely, if the names and addresses appear on a confidential list of bank officers suspected of fraud, the loss may pose a more significant risk of harm.

### *Step 5. Determine the Ability to Mitigate the Risk of Harm.*

The degree of harm will depend on the ability of the Corporation to mitigate further compromise of the data or system(s) affected by the incident. In addition to containing the incident, the FDIC will take appropriate countermeasures, such as monitoring systems to identify misuse of data and patterns of suspicious behavior. Such measures may not prevent the use of the compromised data for identity theft or other harm, but it may limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

**Figure 6. Output of 5-Factor Risk Assessment: Severity of Breach**


1. The nature of the data elements involved
Severity of Breach
3. The likelihood that PII is accessible and usable
lead to harm

After completing the above five steps, the ISPS Incident Lead and Divisional ISM/IR POC(s) will balance the impact level of each of the five factors to determine the overall severity of the loss. The severity of the incident will dictate the recommended course of action and mitigation measures. Since the nature of the data elements (Step/Factor 1) is a key factor in the risk analysis, this factor should be a starting point for assessing the overall severity of the incident. The decision to provide notification should give greater weight to Step/Factor 3 (i.e., likelihood the data is accessible and useable) and to Step/Factor 4 (i.e., whether the incident may lead to harm). For severe breaches involving financial harm, the DBMT will recommend financial remuneration to the affected individuals and/or entities. Less severe breaches that do not involve the loss of sensitive financial data would only merit a notice of the loss.

## Identity Theft Considerations

Although a data breach may pose many types of harm, special consideration must be given to identity theft. Identity theft has been called the crime of the 21st century, favored, according to law enforcement, for its low risks and high rewards. Not only do identity theft victims have to spend money out of pocket to clear up their records, but they also must devote their time – up to hundreds of hours in some cases – to doing so. In the meantime, victims may be unjustly harassed by debt collectors, denied credit or employment opportunities; they may lose their cars or their homes, or be repeatedly arrested for crimes they did not commit.

In analyzing an incident, the ISPS Incident Lead and Divisional ISM will evaluate whether the information involved in the incident poses a risk of identity theft. Factors for determining whether the information could result in identity theft include:

- The data nature/type. For example, if the incident includes any of the following types or combinations of sensitive PII, the incident may pose a risk of identity theft: Social Security Numbers, government-issued identification numbers (driver's license number, state identification number, passport number, etc.), financial account numbers; name, address or telephone number combined with date of birth, password or mother's maiden name;
- How easy or difficult it would be for an unauthorized person to access the information in light of existing controls. For example, a laptop that contains SSNs that are adequately protected by encryption is less likely to be accessed than an unprotected paper file containing SSNs.
- How the loss occurred, including whether it was a result of a criminal act or is likely to result in criminal activity. For example, the risk of identity theft is greater if a thief targeted and stole the data, as opposed to information that was mistakenly left unprotected in a public location.
- The ability of the Corporation or other affected entities to mitigate identity theft by, for example, monitoring for and preventing attempts to misuse the compromised information. For example, alerting financial institutions in incidents involving financial account information can allow them to monitor or close compromised accounts before identity theft is perpetrated.
- Evidence that the breached information is being used to commit identity theft or has been sold.

## Categorizing Incidents Posing a Risk of Identity Theft

As noted, the potential impact/severity of an incident will be categorized as Low, Moderate or High in accord with the standards outlined at the beginning of this appendix. For incidents that pose identity theft concerns, the FDIC applies the following standards:

The potential impact/risk of harm is **LOW** when the risk of identity theft or other harm is unlikely or nonexistent. An incident may be assigned a **LOW** potential impact when, for example:

- The compromise of information could not lead to identity theft or other risk of harm;
- The data elements/type of information could not be used to perpetrate identity theft;
- The information was encrypted; or
- The information has been recovered and determined that there was no access or distribution of the information.

The potential impact/risk of harm is **MODERATE or HIGH** when the risk of identity theft or other harm is likely. An incident may be assigned a **MODERATE or HIGH** potential impact when, for example:

- The compromise of information could lead to identity theft or other risk of harm;
- The data elements/type of information could be used to perpetrate identity theft (e.g., SSN);
- The information was not encrypted or protected;
- The information was targeted and/or determined to be accessed and distributed by unauthorized parties; and/or
- Criminal activity is suspected or confirmed.

In general, the FDIC provides external notification and credit monitoring for MODERATE or HIGH incidents where SSNs or other sensitive information that could lead to identity theft has been compromised.

# APPENDIX L: INCIDENT RISK ANALYSIS (IRA) TEMPLATE

**Standard IRA Template**: The purpose of the standard Incident Risk Analysis (IRA) template is to assess and assign an overall potential impact/severity level (Low, Moderate, or High) to an actual or potential FDIC data breach. In addition, the IRA template is used to determine and document corrective actions and recommended mitigation measures, including whether external notification is recommended, to mitigate the harm posed by the incident. Review the guidance in Appendix K for additional information in making this determination. To review and download the standard IRA template, visit FDIC's internal Privacy Program Forms and Templates webpage located at:

(b)(2),(b)(5) [redacted]

**Specialized IRA Template for Encrypted Devices & Tokens**: ISPS has developed a specialized, pre-populated Incident Risk Analysis (IRA) for use with the following types of incidents, which it has determined bear an inherently low to non-existent risk of harm:

- A lost or stolen laptop, Blackberry, or other FDIC-issued device that is properly secured using an FDIC-approved encryption protocol (e.g., Entrust, PKZip, etc.) and that does not appear to have been targeted for the data contained on the device; or
- A lost or stolen Safeword token, without FDIC credentials accompanying it, that does not appear to have been targeted.

ISPS has authorized the Computer Security Incident Response Team (CSIRT) to close all such incidents upon containment and attach a completed IRA for Encrypted Devices & Tokens to the close-out notification. However, as a best practice and depending on the circumstances of the incident, ISMs and Divisional IR POCs may opt to complete a review of such incidents, follow up with users for educational purposes, and modify the pre-populated IRA for Encrypted Devices & Tokens, as appropriate. The IRA template for Encrypted Devices & Tokens is available for download on the FDIC's internal Privacy Program Forms and Templates webpage located at:

(b)(2),(b)(5) [redacted]

# APPENDIX M: DATA BREACH CLOSE-OUT TEMPLATES

Upon the conclusion of the incident investigation and assessment, the following templates may be used to close out the incident or breach, as well as prepare the Breach Close-Out Summary/Report for the CIO/CPO.

## Sample Incident Close-Out Email (for use by ISM or Designee)

From: ISM or designee
To: ISPS Incident Lead
(b)(2),(b)(5) Cc: [redacted]

Subject: **Incident #:** ____; **Title of Incident:** ______;

**Narrative for Breach:**

This is to inform you that the [insert Division name] has completed its responsibilities as outlined in *FDIC's Data Breach Response Procedures*, dated _____. Since the meeting of the Data Breach Management Team (DBMT), the following steps have been taken to close out this incident [insert list of key action items, such as sending of notification letters to affected individuals with the offer of credit monitoring]: It is recommended that the breach can be closed with CSIRT by the ISPS Incident Lead.

**Narrative for Non-Breach**:

This is to inform you that [insert Division name] has completed its responsibilities as outlined in *FDIC's Data Breach Response Procedures*, dated _____. [Insert Division name] has taken the following steps to close out this incident [insert list of key action items, such as the sending of FDIC policies and procedures to the individual]: It is recommended that the breach can be closed with CSIRT by the ISPS Incident Lead.

## Sample Incident Concurrence Close-Out Email (for use by ISPS Incident Lead)

From: ISPS Incident Lead
(b)(2),(b)(5) To: FDIC CSIRT [redacted]
(b)(2),(b)(5) Cc: [redacted] Privacy Program Manager; Chief Information Security Officer

Subject: **Incident #:** ____; **Title of Incident:** ______;

The FDIC Information Security and Privacy Staff (ISPS) concurs with the ISM's recommendation below that this incident can be closed. It [was/was not] a [privacy/security] breach as indicated below [attach copy of ISM close-out email and attach any additional, pertinent correspondence that illustrates the nature of the breach and the mitigation strategies]. In addition to the steps outlined below, we will continue to work with [Affected Division/Office] on any post-breach notification activities/issues. Thank you.

## Sample Breach Close-Out Summary / Report (for use by ISPS Incident Lead)

From: ISPS Incident Lead
To: FDIC CIO/CPO
(b)(2),(b)(5) Cc: [redacted] PPM; CISO
Subject: Close-Out Report for **Incident #: ____; Title of Incident:**

Attached is the final Incident Close-Out Summary Report showing all associated DBMT action items with respect to [Title of Incident; Incident #] that occurred in [Month, Year]. All DBMT action items have been completed as indicated in red in the attached Word document.

Also, please find attached copies of the final [Notification Letters that were sent to affected individuals and/or entities or the banks; Cure and Demand letters; and/or other applicable letters generated/ disseminated in response to the breach]. [Provide a brief explanation of the letters and dates on which they were sent].

The attached files are being sent to you for information and/or record keeping only. No action is required. However, If you have any questions regarding this close-out summary, please let me know.

---

**Sample Data Breach Management Team (DBMT) Summary Report Template**
**Date**
**CSIRT INC# (Risk Level Determined by DBMT) CAT# (Affected Division/Office)**
**Brief Description of Incident (e.g., Lost/Stolen Thumb Drive Containing PII)**

**INCIDENT SUMMARY:**

[Provide a summary of the incident based on the CSIRT Report and additional information provided by the Divisional ISM / IR POCs. Include a statement indicating what the DBMT's determination was as to the overall risk of harm/impact and whether a notification to potentially affected individuals/entities was required.] ***[Provide statement in red font indicating that incident was formally closed-out with CSIRT by the ISPS Incident Lead on X Date.]***

**DBMT MEMBERS AND TEAM**

[Name, Title, Division]

**NATURE OF THE DATA ELEMENTS BREACHED**

[Provide summary of the data that was lost and the manner/medium, for example: The stolen USB device contained back-up data of a completed Structured Loan Sales and included sensitive PII relevant to loan applications of bank customers whose loans were being sold. The compromised loan files included 21 Receiverships, span 30 states, and are from a period covering 1986 through 2010. Some of the files contain credit reports and tax returns.]

***[Provide updates in red font regarding the nature of the data based on the outcome of the investigation.]***

**NUMBER OF AFFECTED INDIVIDUALS/ENTITIES**

[There were approximately [Number] affected individuals and/or [Number] affected entities/businesses.] ***[Provide final count of affected individuals/entities based on outcome of investigation.]***

## POSSIBILITY OF MISUSE [LIKELIHOOD THE INFORMATION IS ACCESSIBLE AND USABLE]

[Explain how likely it is that the data is accessible and usable. Key considerations are whether/what type of controls were in place to protect the data, as well as whether the data was intentionally targeted.]

## LIKELIHOOD THE BREACH MAY LEAD TO HARM

[Provide a brief summary regarding the likelihood that the breach may lead to harm.]

## ABILITY OF THE CORPORATION TO MITIGATE THE RISK OF HARM

[Summarize any actions taken to contain, mitigate and recover from incident. Explain the likelihood that the data will be recovered.]

## DBMT FINDINGS/RESULTS

[Explain the overall risk of harm (Low, Moderate or High) based on the above five factors (i.e., nature of data elements, number of affected individuals/entities, possibility of misuse, likelihood incident may lead to harm, and ability of Corporation to mitigate harm).

[In light of this, the DBMT agreed on the following:]

- [Insert bulleted list of DBMT findings and summarize any updates in red font.]

## MITIGATION STRATEGIES & LESSONS LEARNED [IF APPLICABLE]

[The following mitigation strategies and lessons learned, if applicable, were identified by the DBMT in an effort to preclude future occurrence of similar incidents:]

- [Insert bulleted list of mitigation strategies and lessons learned, if applicable. Summarize any updates in red font.]

# APPENDIX N: GLOSSARY OF TERMS AND DEFINITIONS

1. **Access***:* The ability or opportunity to gain knowledge of personally identifiable information.

2. **Agency and Business Sensitive Information (BSI):** Identifying information about the Corporation, another government agency, a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices or other crimes, such as bank account information, trade secrets, confidential or proprietary business information. Commercial information is not confined to records that reveal basic commercial operations, but includes any information in which the submitter has a commercial interest, and may include information submitted by a nonprofit entity. Other terms for BSI that must be protected from disclosure are: "confidential business information," "business identifiable information," "confidential commercial information," and "proprietary information."

3. **Breach***:* The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to agency or business sensitive information and/or personally identifiable information in usable form, whether physical or electronic. A breach would not occur if, for example, the information was properly encrypted within a mobile computing device because the information would be unusable.

4. **Incident**: An occurrence that potentially or actually jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, acceptable use policies or standard computer security practices. This guide focuses on two categories of incidents:

    i. **Computer Security Incident**: An event that threatens the security of the FDIC Automated Information System (AIS), which includes FDIC's computers, mainframe, networks, software and associated equipment, and information stored or transmitted using that equipment. For example:

        1. Attempts by unauthorized individuals to gain access to FDIC automated information systems, computer applications, or data. This would include everything from hacker attempts, to someone trying to steal passwords and user ids, to someone trying to use an employee's workstation without the employee's knowledge.
        2. Any attempt by someone to gain access to FDIC data when they are not authorized to view it.
        3. Any event, intentional or not, that results in damage, corruption, misuse, or unauthorized exposure of FDIC data.
        4. Any attempt to interfere with normal FDIC AIS operations so as to interfere with FDIC work or with other FDIC operations that depend upon the FDIC AIS. This includes virus or worm attacks and denial of service attacks that limit or prevent use of the FDIC AIS, as well as any unauthorized modification of FDIC software. It also includes interference with the PBX (Voice telecommunications) system, since it depends upon computers.
        5. Theft or vandalism of FDIC AIS related equipment, such as PCs, disks, software, modems, servers, smartcards, printouts of sensitive information, and PBX equipment. (These should be reported both to Physical Security and CSIRT.)
        6. Theft of FDIC AIS related services, e.g., telephone fraud, theft of computer time.
        7. Any other violation of computer security policy.

    ii. **Physical Security Incident**: The known or suspected loss or compromise of a physical asset, equipment or file containing sensitive information. For example: loss/theft of a laptop, Blackberry, thumb drive, mail shipment, box, fax, printout, etc. that contains sensitive information.

5. **Harm:** Damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

6. **Mitigation**: To make less severe, to partially remove, or to correct, so that harmful potential effects of an incident are reduced or eliminated.

7. **Personal Identifiable Information (PII)**: Any information about an individual maintained by FDIC which can be used to distinguish or trace that individual's identity, such as their full name, home address, E-mail address (non-work), telephone numbers (non-work), Social Security Number (SSN), driver's license/state identification number, employee identification number, date and place of birth, mother's maiden name, photograph, biometric records (e.g., fingerprint, voice print), etc. This also includes, but is not limited to, education, financial information (e.g., account number, access or security code, password, personal identification number,) medical information, investigation report or database, criminal or employment history or information, or any other personal information which is linked or linkable to an individual.

8. **Privacy:** The right to be left alone and to control the conditions under which information pertaining to a person is collected, maintained, used and disseminated. Privacy is the state of being free from unsanctioned intrusion. As an issue, privacy pertains to personal information-data that can be linked to an individual human being. In other words, all personal information requires privacy considerations. When handling personal data of any kind, it is important to take steps to assure privacy of the information. Privacy is both a good practice and mandated by law.

9. **Professional Need to Know**: Specific and limited information necessary to complete assigned work, in the case of performing official business.

10. **Security**: Administrative, physical and technical safeguards, used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, to maintain the integrity of the information.

11. **Security Incident**: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

12. **Sensitive information**: Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. It includes the following:

    a. Information that is exempt from disclosure under the Freedom of Information Act (FOIA) such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports (see FDIC Rules and Regulations, 12 C.F.R. Part 309, for further information);

    b. Information under the control of FDIC contained in a Privacy Act system of record that is retrieved using an individual's name or by other criteria that identifies an individual (see FDIC Rules and Regulations, 12 C.F.R. Part 310, for further information);

    c. PII about individuals maintained by FDIC that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (e.g., SSN) or a combination of two or more items (e.g., full name along with, financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud; and

    d. Information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities.

10. **Violation**: Infraction of a law; going against established rules.

    *Examples of Violations*

    1. Misuse of computer access passwords (i.e., sharing or posting passwords, unauthorized use of others' accounts, allowing use of accounts by others, etc.)
    2. Attempting to bypass or exploit physical or technical information security measures.
    3. Accessing BSI and/or PII outside of your "Professional Need To Know", either for personal curiosity or as a "favor" for someone else.
    4. Storing unencrypted BSI and/or PII on removable/portable computer media/devices, laptops, remote workstations, (disks, CD's, tapes, keys, etc.)
    5. Unauthorized publication of BSI and/or PII in any medium.
    6. Selling BSI and/or PII or inappropriately giving such information to the news media or other unauthorized recipients.
    7. Unauthorized disclosure of BSI and/or PII to persons without a "Need to Know" either deliberately or accidentally (i.e., discussing BSI/PII in public places, leaving documents containing BSI/PII unattended in public places, posting BSI/PII on unsecured web-sites, "misplacing" or otherwise losing unencrypted BSI/PII stored on removable computer media, etc.).

# APPENDIX O – WHEN IS AN INCIDENT A BREACH?

This appendix provides definitions and guidance to help distinguish between a data incident and a data breach.

## *Definitions*

A data incident is the **suspected or confirmed** loss, theft, or unauthorized acquisition or disclosure of sensitive information, whether in hardcopy/paper or electronic form.

A data breach is the **actual confirmed** loss or unauthorized acquisition or disclosure of sensitive information that jeopardizes FDIC's mission or poses a risk of harm to an individual or entity.

## *Methodology*

Based on the above definitions, all breaches start as incidents, but not all incidents are breaches. In determining whether an incident constitutes a data breach, the first step is to consider whether sensitive information was compromised using the following four factor methodology:

1. **Information Type** – The first factor to consider is the type of the information involved in the incident. Questions to consider include:
   - Is the information identifiable?
   - How sensitive is the information?

2. **Information Recipient** – The second factor is the recipient of the information and whether they are authorized to view/access the information and whether they have any known or potential motivations to misuse the information. Questions to consider include:
   - Who received or obtained the information?
   - Does the recipient have a legitimate "need to know" or business purpose for receiving or accessing this information? Is the recipient of the data legally or contractually required to protect the information?
   - Was the data given to or obtained by someone who has no motivation to potentially misuse the information? Or, was it given to or obtained by someone who either intentionally targeted the information for identity theft or to perpetrate other harm, or by someone who has a potential motivation to abuse the information?

3. **Information Safeguards and Mitigation** – The third factor involves whether there are any mitigation steps taken by the Corporation or whether there are any existing safeguards in place, such as encryption, to protect the data from compromise. Questions to consider include:
   - Based on actions taken after the disclosure, was FDIC able to stop any potential compromise, such as getting the information back or obtaining assurances that the information was destroyed before it was improperly further used or disclosed?
   - Were there any existing safeguards in place to adequately protect the data from unauthorized access or compromise? For example, if an FDIC laptop or device containing sensitive information was stolen, was the information appropriately secured using an FDIC-approved encryption protocol (e.g. [redacted]

(b)(2),(b)(5)

4. **Information Access or Compromise** – The final factor is whether the information was actually accessed or viewed by unauthorized parties or for unauthorized purposes. For example, looking at forensic evidence, if available, FDIC may be able to ascertain whether information recovered was actually accessed or viewed. For incidents that involve a lost or stolen device, the

FDIC does not consider the information contained on the device to have been compromised/breached, if the device or data was adequately encrypted.

In summary, it is important to be consistent in determining whether an incident resulted in financial, reputational or other harm to FDIC and/or to affected individuals/entities, and to use common sense. For example, agencies must avoid over-notifying individuals, particularly if there will be no potential adverse impact whatsoever. On the other hand, when applying the above methodology and it is determined that notification is not required, but common sense would dictate that the individual/entity should know about the incident because there may be some actions that they may need to take, then FDIC must use a best judgment approach and take the prudent course of action.

## DESCRIPTION OF FDIC'S PRIVACY PROGRAM AND TRAINING

The Federal Deposit Insurance Corporation (FDIC) has established a risk-based, agency-wide Privacy Program within the Chief Information Officer Organization (CIOO). The FDIC Chief Information Officer (CIO) also serves as the Chief Privacy Officer (CPO) and reports directly to the FDIC Chairman. The CPO is responsible for the implementation and oversight of the privacy program and for managing a comprehensive set of privacy and data protection policies and procedures designed to promote robust and effective privacy protection throughout the agency. The privacy program includes routine privacy awareness activities and training for employees and contractors.

Operating under federal laws and regulations, it is the responsibility of the FDIC and each employee and contractor to protect the privacy rights of individuals and to protect personally identifiable information (PII) from unauthorized use, access, disclosure, sharing, or disposal. In support of these mandates, the FDIC completed the following privacy awareness and training activities this reporting year:

- New hires at the FDIC underwent an extensive orientation that includes review of the agency's privacy policies and guidelines, emphasizing employees' responsibilities.

- As part of the on-boarding orientation, new hires were provided a booklet entitled*: A Guide for the FDIC - Protecting Sensitive Information in Your Work Area.*

- Awareness efforts are conducted annually throughout the agency using privacy awareness campaigns in both paper and electronic media. This year, the FDIC centered its awareness campaign around the theme *Privacy - No Appetite for Risk,* which focused on reducing privacy risk by protecting sensitive information (SI), including PII entrusted to the agency. The awareness campaign efforts included a global message distributed to all employees and contractors, lobby posters and bulletins displayed at all FDIC offices nationwide, and privacy tips imprinted on employees' earnings and leave statements and posted on TV monitors nationwide. The campaign messaging centered on four simple reminders to reduce overall privacy risk:

    - The secure handling of SI/PII
    - How to exercise control when sharing SI/PII
    - Minimizing risk through the observation of sound PII protection business practices
    - Emphasis on "think before you click" philosophy

- FDIC participated in the Global Privacy Day on January 28th with an agency-wide distribution of a global message and display of graphic material in support of the global initiative to raise privacy awareness and promote privacy and data protection best practices.

- During this reporting period, FDIC conducted five (5) unannounced privacy compliance walkthrough assessments at the following FDIC Regional Offices: New York, San Francisco, Atlanta, Kansas City, and Chicago. These walkthrough assessments raise privacy awareness through written reports detailing incidents observed surrounding the handling of FDIC data. Where necessary, FDIC provides targeted training to divisions and offices on how to further enhance PII protections and handling practices.

- Privacy awareness is included in the agency's training of contract oversight managers and technical monitors at FDIC's headquarters and the Dallas Regional Office.

- Targeted training was prepared and provided to divisions' oversight managers on the preparation of privacy impact assessments for outsourced vendors.

- Privacy program, along with security and legal staff conducted nationwide training via the *Privacy and Data Protection Roadshow Regional Tours.* The roadshows were conducted in the New York, Boston, San Francisco, Atlanta, Kansas City, and Chicago regional offices and centered on the following four key privacy and data protection issues impacting FDIC employees' and contractors' work and home lives:

  - Privacy Act 101: How to Avoid Privacy and Legal Pitfalls
  - Staying out of the Headlines: The Top Ten Things You Can Do to Prevent an FDIC Data Breach
  - Cybersecurity for Managers and Employees: Reducing the Agency's Appetite for Risk
  - Starting Privacy Early: Lowering Your Online Profile Risk

- Lastly, through FDIC Circular 1360.16, Mandatory Information Security Awareness Training, FDIC requires annual information security and privacy awareness training for all employees and contractors who manage, use, or operate a federal computer system within or under the supervision of FDIC. Each FDIC employee and contractor must annually review and complete the information security and privacy awareness web-based training course and affirm his or her understanding of their responsibilities. This mandatory training is intended to provide employees and contractors with the knowledge necessary to support FDIC's ongoing efforts to comply with key laws and regulations governing the agency's collection, use, sharing, and protection of sensitive data. This training also instructs on how to maintain the confidentiality, integrity, and availability of the FDIC's network, systems, software, and data.

# Inspector General

Section Report

2015

Annual FISMA Report

## Federal Deposit Insurance Corporation

## Section 1: Continuous Monitoring Management

**1.1 Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.**

**1.1.1 Please provide the D/A ISCM maturity level for the People domain.**

**Ad Hoc (Level 1)**

**Comments:** As discussed in our report, the FDIC needed to complete a comprehensive assessment of the role of the Information Security Managers (ISMs) in managing information security risks, including implementation of the ISCM program, within the FDIC's Divisions and Offices. The FDIC then needs to establish a plan to ensure the ISM role has the skills, resources, training, reporting lines, and performance measurements necessary to fulfill their assigned duties and effectively manage information security risks.

**1.1.2 Please provide the D/A ISCM maturity level for the Processes domain.**

**Ad Hoc (Level 1)**

**Comments:** As discussed in our report, GAO noted in its July 2014 report, Information Security, FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain (2014 Security Report) that the FDIC had not defined standard baseline configurations for many of its information systems. At the close of our audit, the FDIC was still working to define these baselines as part of a multi-year project to document, implement, and monitor against approved baseline configurations in support of its ISCM program. Management continued to make progress in this area and plans to be substantially complete by the end of 2016.

**1.1.3 Please provide the D/A ISCM maturity level for the Technology domain**

**Ad Hoc (Level 1)**

(b)(5),(b)(7)(E) **Comments:**

**1.1.4 Please provide the D/A ISCM maturity level for the ISCM Program Overall.**

**Ad Hoc (Level 1)**

**1.2 Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.**

**See OIG FISMA performance audit report.**

## Section 2: Configuration Management

For Official Use Only

## Section 2: Configuration Management

**2.1 Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**No**

**2.1.1 Documented policies and procedures for configuration management.**

**Yes**

**2.1.2 Defined standard baseline configurations.**

**No**

**Comments:** As discussed in our report, GAO noted in its 2014 Security Report that the FDIC had not defined standard baseline configurations for many of its information systems. At the close of our audit, the FDIC was working to define these baselines as part of a multi-year project to document, implement, and monitor configurations against approved baselines. Management continues to make progress in this area and plans to be substantially complete by the end of 2016.

**2.1.3 Assessments of compliance with baseline configurations.**

**No**

**2.1.4 Process for timely (as specified in organization policy or standards) remediation of scan result findings.**

**Yes**

**2.1.5 For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.**

**Yes**

**2.1.6 Documented proposed or actual changes to hardware and software baseline configurations.**

**No**

**Comments:** Although the FDIC had a process in place for documenting proposed or actual changes to approved baseline configurations, management had not yet defined these baselines.

**2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).**

**Yes**

## Section 2: Configuration Management

2.1.8 Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in organization policy or standards. (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2).

(b)(5),(b)(7)(E) No

[redacted]

2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).

Yes

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

See OIG FISMA performance audit report.

2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

(b)(5),(b)(7)(E)

No

[redacted]

2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.

No

## Section 3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

Yes

3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).

Yes

## Section 3: Identity and Access Management

3.1.2 **Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).**

**Yes**

3.1.3 **Organization has planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).**

**No**

**Comments:** The FDIC is not subject to HSPD-12. However, the FDIC had recently decided to implement a USB token-based multi-factor authentication for logical access across the organization.

3.1.4 **Organization has planned for implementation of PIV for physical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).**

**No**

**Comments:** The FDIC is not subject to HSPD-12. However, the FDIC had issued PIV cards to just over half of its employee and contractor personnel as of May 2015 when the Corporation decided to "pause" PIV card issuance until it could adequately reassess the costs, benefits, and risks of using the General Service Administration's USAccess program.

3.1.5 **Ensures that the users are granted access based on needs and separation-of-duties principles.**

**Yes**

3.1.6 **Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).**

**Yes**

3.1.7 **Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.**

**No**

**Comments:** As discussed in our report, access reviews were not always completed in a timely manner. Also, privileged user access for contractor personnel was not always deactivated in a timely manner when no longer needed.

3.1.8 **Identifies and controls use of shared accounts.**

**Yes**

**Comments:** We found that the FDIC generally identified and controlled the use of shared accounts. However, as discussed in our report, the FDIC did not properly control a shared User ID and password for an outsourced information service.

## Section 3: Identity and Access Management

3.2 **Please provide any additional information on the effectiveness of the organization's Identity and Access Management Program that was not noted in the questions above.**

**See OIG FISMA performance audit report.**

## Section 4: Incident Response and Reporting

4.1 **Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**Yes**

4.1.1 **Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).**

**Yes**

4.1.2 **Comprehensive analysis, validation, and documentation of incidents.**

**Yes**

4.1.3 **When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).**

**Yes**

4.1.4 **When applicable, reports to law enforcement and the agency Inspector General within established timeframes.**

**Yes**

4.1.5 **Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).**

**Yes**

4.1.6 **Is capable of correlating incidents.**

**Yes**

4.1.7 **Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).**

**Yes**

## Section 4: Incident Response and Reporting

4.2 **Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.**

**See OIG FISMA performance audit report.**

## Section 5: Risk Management

5.1 **Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**Yes**

5.1.1 **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.**

**Yes**

5.1.2 **Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800- 37, Rev. 1.**

**No**

**Comments:** As discussed in our report, we found weaknesses in the ISM role, which is responsible for managing information security risks from a mission and business process perspective within the FDIC's Divisions and Offices.

5.1.3 **Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev.1.**

**No**

**Comments:** As discussed in our report, we found weaknesses in the ISM role, which is responsible for managing information security risks from a mission and business process perspective within the FDIC's Divisions and Offices.

5.1.4 **Has an up-to-date system inventory.**

**Yes**

5.1.5 **Categorizes information systems in accordance with government policies.**

**Yes**

## Section 5: Risk Management

5.1.6 **Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

**Yes**

**Comments:** The FDIC is currently working to adopt new or modified security controls, as appropriate, consistent with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4.

5.1.7 **Implements the approved set of tailored baseline security controls specified in metric 5.1.6.**

**Yes**

**Comments:** The FDIC is currently working to adopt new or modified security controls, as appropriate, consistent with NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4.

5.1.8 **Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.**

**Yes**

5.1.9 **Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.**

**Yes**

5.1.10 **Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.**

**Yes**

5.1.11 **Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).**

**Yes**

5.1.12 **Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.**

**Yes**

## Section 5: Risk Management

5.1.13 **Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).**

**Yes**

5.1.14 **The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.**

**Yes**

5.1.15 **For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.**

**Yes**

5.2 **Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.**

**See OIG FISMA performance audit report.**

## Section 6: Security Training

6.1 **Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**Yes**

6.1.1 **Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).**

**Yes**

6.1.2 **Documented policies and procedures for specialized training for users with significant information security responsibilities.**

**No**

**Comments:** The FDIC had not developed and mandated role-based training for the ISMs to ensure that they understand their assigned duties and continue to maintain the skillsets needed to effectively fulfill their role.

6.1.3 **Security training content based on the organization and roles, as specified in organization policy or standards.**

**Yes**

## Section 6: Security Training

6.1.4 **Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.**

**Yes**

6.1.5 **Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.**

**Yes**

6.1.6 **Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).**

**Yes**

6.2 **Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.**

**See OIG FISMA performance audit report.**

## Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**Yes**

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.**

**Yes**

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

**Yes**

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

**Yes**

7.1.4 **Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.**

**Yes**

## Section 7: Plan Of Action & Milestones (POA&M)

**7.1.5** **Ensures resources and ownership are provided for correcting weaknesses.**

**Yes**

**7.1.6** **POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk- based decision to not implement a security control) (OMB M-04-25).**

**Yes**

**7.1.7** **Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).**

**No**

**Comments:** The FDIC estimated the security costs for remediating security vulnerabilities in the aggregate, but not for specific information systems or individual vulnerabilities in a POA&M.

**7.1.8** **Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53:CA-5; OMB M-04-25).**

**Yes**

**7.2** **Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.**

**See OIG FISMA performance audit report.**

## Section 8: Remote Access Management

**8.1** **Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

**Yes**

**8.1.1** **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).**

**Yes**

**8.1.2** **Protects against unauthorized connections or subversion of authorized connections.**

**Yes**

## Section 8: Remote Access Management

8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).

Yes

8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).

Yes

8.1.5 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

8.1.6 Defines and implements encryption requirements for information transmitted across public networks.

Yes

8.1.7 Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

Yes

8.1.8 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).

Yes

8.1.9 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).

Yes

8.1.10 Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).

Yes

8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.

See OIG FISMA performance audit report.

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

## Section 9: Contingency Planning

## Section 9: Contingency Planning

**9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

**9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).**

Yes

**9.1.2 The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).**

No

(b)(5),(b)(7)(E)

**Comments:** The FDIC is currently working to address potential gaps that may exist between the 12-hour timeframe required to restore mission essential functions following an emergency and [redacted] recovery time objective for restoring mission-critical applications.

**9.1.3 Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).**

Yes

**9.1.4 Testing of system-specific contingency plans.**

Yes

**9.1.5 The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).**

Yes

**9.1.6 Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

**9.1.7 Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.**

Yes

**9.1.8 After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).**

Yes

## Section 9: Contingency Planning

9.1.9 Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).

(b)(5),(b)(7)(E) No

[redacted]

9.1.10 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

9.1.11 Contingency planning that considers supply chain threats.

Yes

9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

See OIG FISMA performance audit report.

## Section 10: Contractor Systems

10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

10.1.1 Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.

Yes

10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).

(b)(5),(b)(7)(E) No

Comments: [redacted]

## Section 10: Contractor Systems

10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.

Yes

10.1.4 The inventory identifies interfaces between these systems and organization- operated systems (NIST SP 800-53: PM-5).

Yes

10.1.5 The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

10.2 Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.

See OIG FISMA performance audit report.

# Office of Inspector General

Office of Audits and Evaluations
Report No. AUD-16-001

## Audit of the FDIC's Information Security Program—2015

**This report contains sensitive information and is for official use only. Other than the Executive Summary, the contents of the report are not releasable without the approval of the Office of Inspector General.**

October 2015

**Executive Summary**

# Office of Inspector General

## Audit of the FDIC's Information Security Program—2015

Report No. AUD-16-001
October 2015

## Why We Did The Audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices and to report the results to the Office of Management and Budget (OMB). This Act replaced provisions of the Federal Information Security Management Act of 2002. FISMA states that the independent evaluations are to be performed by the agency Inspector General (IG), or an independent external auditor as determined by the IG. The FDIC Office of Inspector General (OIG) engaged the professional services firm of Cotton & Company LLP (C&C) to conduct a performance audit to satisfy this FISMA requirement.

The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices. To address the objective, C&C performed audit procedures to evaluate the 10 security control areas outlined in the Department of Homeland Security's (DHS) June 19, 2015, document entitled, *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*. C&C's work included an analysis of selected security controls related to two of the FDIC's general support systems and two major applications, as well as a review of the Corporation's risk management activities related to an outsourced information service provider that facilitated employee recruitment efforts.

## Background

FISMA requires federal agencies to develop, document, and implement agency-wide information security programs to provide security for their information and information systems and to support the operations and assets of the agencies, including information and information systems that are provided or managed by another agency, contractor, or other source. FISMA directs the National Institute of Standards and Technology (NIST) to develop risk-based standards and guidelines to assist agencies in defining security requirements for their information systems. In addition, OMB issues information security policies and guidelines for federal information resources pursuant to various statutory authorities. Further, under FISMA, and in consultation with OMB, DHS administers the implementation of agency information security policies and practices for information systems. DHS's responsibilities include developing operational directives regarding such matters as reporting security incidents and providing operational and technical assistance to agencies in implementing information security-related guidance.

## Audit Results

Overall, C&C concluded that, except as described below, the FDIC's information security program and practices were generally effective. As part of the firm's work, C&C noted several important improvements in the FDIC's information security program over the last year. Specifically, the FDIC:

- enhanced its patch and vulnerability management program through the creation of a Patch and Vulnerability Management Group (PVG) and related subgroups that meet regularly to evaluate technical vulnerabilities in the FDIC's Information Technology (IT) environment and work to implement solutions;

- improved its process for managing known security weaknesses through Plans of Actions and Milestones (POA&Ms) as demonstrated by a reduction in the number of open high-risk POA&Ms from 49 in September 2014 to 26 in August 2015;

- expanded its security metrics reporting, particularly to senior management, which has resulted in increased awareness of information security risks and enabled management to take more proactive measures to improve the FDIC's overall information security posture; and

- revised its corporate information security risk management program policy to better align with NIST guidance.

In addition, the FDIC implemented five of seven previously unaddressed recommendations from our 2013 and 2014 security evaluation reports required by FISMA, and was working to address the remaining two recommendations at the close of the audit.

Notwithstanding these accomplishments, C&C identified aspects of the FDIC's information security program warranting management attention. Of particular note, the duties and role of the FDIC's Information Security Managers (ISM) in addressing information security requirements and risks within the FDIC's business divisions and offices have evolved since the ISM program was established. However, the FDIC had not recently completed a comprehensive assessment to determine whether the skills, training, oversight, and resource allocations pertaining to the ISMs enable them to effectively carry out their increased responsibilities and address security risks within their divisions and offices. In addition, the FDIC had not always ensured the timely completion of outsourced information service provider assessments or the timely review of user access to FDIC information systems. Further, the FDIC had not identified access control weaknesses for an outsourced information service provider that C&C found during its audit.

The FDIC was continuing its work on a multi-year initiative to develop secure baseline configurations for its information systems. Baseline configurations that are documented, implemented, and monitored are a critical control for ensuring that the FDIC's information systems are adequately protected. The FDIC was also working to implement multifactor authentication for nonprivileged network users and, separately, to perform system event logging and monitoring for certain databases. Continued management attention on each of these initiatives is warranted to ensure their success. C&C identified additional findings in the security control areas of risk management and configuration management that are described in the firm's report.

Finally, C&C noted that the FDIC depended heavily upon its infrastructure services contract (ISC) to support IT operations and implement security controls. C&C noted certain risks associated with the ISC, that, if not properly managed, could negatively impact the FDIC's IT operations, including its security operations. FDIC officials informed C&C that they were aware of these risks and were taking steps to mitigate them.

## Recommendations and Corporation Comments

The report contains five recommendations addressed to the Acting Chief Information Officer (CIO) and one recommendation addressed to the Director, Division of Administration (DOA), that are intended to improve the effectiveness of the FDIC's information security program controls and practices. The Acting CIO and Director, DOA, provided a joint written response, dated October 23, 2015, to a draft of C&C's report. In the response, FDIC management concurred with all six of the report's recommendations and described planned and completed actions that were responsive to the recommendations.

C&C identified certain other matters during the audit that the firm did not consider significant in the context of the audit objective. The OIG plans to communicate these matters separately to appropriate FDIC management officials.

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

FDIC
**Federal Deposit Insurance Corporation**
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits and Evaluations
Office of Inspector General

**DATE:** October 28, 2015

**MEMORANDUM TO:** Martin D. Henning
Acting Chief Information Officer

Arleas Upton Kea
Director, Division of Administration

**/Signed/**

**FROM:** Mark F. Mulholland
Assistant Inspector General for Audits

**SUBJECT:** *Audit of the FDIC's Information Security Program–2015*
(Report No. AUD-16-001)

The subject final report is provided for your information and use. Please refer to the Executive Summary, included in the report, for the overall audit results. Your comments on a draft of this report were responsive to the recommendations. Our evaluation of your response is incorporated into the body of the report.

Consistent with the agreed-upon approach to the Corrective Action Closure (CAC) process, the Office of Inspector General (OIG) plans to limit its review of CAC documentation to those recommendations that we determine to be particularly significant. Such determinations will be made when Corporate Management Control (CMC) advises us that corrective action for a recommendation has been completed. Recommendations deemed to be significant will remain open in the OIG's System for Tracking and Reporting (STAR) until we determine that corrective actions are responsive. All other recommendations will be closed in STAR upon notification by CMC that corrective action is complete, but will remain subject to follow-up at a later date.

**This report contains sensitive information and is for official use only. We do not intend to make this report available to the public in its entirety. The report's Executive Summary, which does not contain sensitive information, will be posted on our public Web site. We request that you safeguard the contents of the report accordingly.**

If you have questions concerning the report, please contact me at (703) 562-6316 or Joseph E. Nelson, Information Technology Audit Manager, at (703) 562-6314. We appreciate the courtesies extended to the OIG and contractor staff.

Attachment

## *Table of Contents*

**Part I**

**Part II**

# *Part I*

# *Report by Cotton & Company LLP*

# Audit of the Federal Deposit Insurance Corporation's Information Security Program – 2015

October 28, 2015

Cotton
Company

Cotton & Company LLP
635 Slaters Lane
Alexandria, Virginia 22314
(b)(4) 703.836.6701 | [redacted]
(b)(4),(b)(6) [redacted] | www.cottoncpa.com

## TABLE OF CONTENTS

Cotton & Company

635 Slaters Lane
4th Floor
Alexandria, VA 22314

P [redacted] (b)(4),(b)(6)
F
www.cottoncpa.com

October 28, 2015

Mark F. Mulholland
Assistant Inspector General for Audits
Office of the Inspector General
Federal Deposit Insurance Corporation

Subject: Audit of the Federal Deposit Insurance Corporation's Information Security Program

Cotton & Company LLP is pleased to submit the attached report detailing the results of our performance audit of the Federal Deposit Insurance Corporation's (FDIC) information security program. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including the FDIC, to perform annual independent evaluations of their information security programs and practices. FISMA states that the evaluations are to be performed by the agency Inspector General (IG), or an independent external auditor as determined by the IG. The FDIC Office of Inspector General engaged Cotton & Company LLP to conduct this audit pursuant to Contract Number CORHQ-15-G-0161. Cotton & Company LLP performed the work from June through September 2015.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Sincerely,
Cotton & Company LLP

(b)(4),(b)(6) [redacted]

Loren Schwartz, CPA, CISSP, CISA
Partner, Information Assurance

*Sensitive Information—For Official Use Only*

## Introduction

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA) (Public Law (P.L.) No. 113-283).[1] FISMA requires agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of the management, operational, and technical controls over information technology (IT) that support agency operations and assets.

FISMA replaced relevant portions of the Federal Information Security Management Act of 2002 (P.L. 107-347). While both versions of the legislation required agencies to conduct an annual independent evaluation under the authority of the Inspector General (IG) and required IGs to assess the effectiveness of their agency's information security program, FISMA no longer requires the evaluation to include an assessment of the program's compliance with FISMA and other IT-related requirements.

## Objective

The objective of this performance audit was to evaluate the effectiveness of the FDIC's information security program and practices.

## Scope and Methodology

Cotton & Company LLP conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management officials throughout the audit.

To accomplish our objective, we:

- Evaluated the FDIC's information security program, plans, policies, and procedures in place as of September 1, 2015, for consistency with applicable federal laws; policy and guidance issued by the Office of Management and Budget (OMB); and security standards and guidelines published by the National Institute of Standards and Technology (NIST).
- Performed detailed audit procedures to address the questions contained in the Department of Homeland Security's (DHS) June 19, 2015, document entitled *FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics*. The questions contained in this document cover the following ten areas:

  (i) Continuous Monitoring Management
  (ii) Configuration Management
  (iii) Identity and Access Management
  (iv) Incident Response and Reporting

[1] The FDIC determined that the 2014 version of the FISMA legislation is legally binding on the FDIC.

(v) Risk Management
(vi) Security Training
(vii) Plan of Action & Milestones (POA&M)
(viii) Remote Access Management
(ix) Contingency Planning
(x) Contractor Systems

- Selected a non-statistical sample[2] of the following information systems and outsourced information service provider to support our analysis, findings, and conclusions:

(b)(5)

  - [redacted]

- Conducted interviews with personnel from the Division of Information Technology (DIT) and Information Security and Privacy Staff (ISPS), as well as with individuals serving as Information Security Managers (ISM) throughout the FDIC.
- Reviewed information security policies, procedures, and practices for consistency with NIST and OMB guidance; reviewed system documentation and other relevant information; and conducted testing on selected higher-risk controls.

Cotton & Company LLP conducted the audit onsite at the FDIC's Virginia Square location in Arlington, Virginia. We performed fieldwork from June through September 2015.

## BACKGROUND

The FDIC is an independent agency created by the Congress to maintain stability and public confidence in the nation's financial system by:

- Insuring deposits,
- Examining and supervising financial institutions for safety and soundness and consumer protection,
- Conducting risk analysis and prudential supervision of systemically important financial institutions, and
- Managing receiverships

Congress created the FDIC through the Banking Act of 1933. Among other things, the statute provided a federal government guarantee of deposits in U.S. depository institutions so that depositors' funds, within certain limits, would be safe and available to them in the event of a financial institution failure. In addition to its role as insurer, the FDIC is the primary federal regulator of federally insured state-chartered banks that are not members of the Federal Reserve System. The FDIC also acts as receiver for insured depository institutions that fail and has resolution-planning responsibilities (jointly with the

[2] Non-statistical samples are judgmental and cannot be projected to the population.

Board of Governors of the Federal Reserve System) for large and complex financial companies covered under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act).

## Nature of the Organization

The FDIC is a mixed-ownership government corporation. As such, it is not always legally subject to the same laws, regulations, and policy statements as are other executive-branch agencies.

## Overview of the FDIC's Information Security Program

The FDIC's Board of Directors has ultimate responsibility for the security of the FDIC's information and information systems. The FDIC's Chief Information Officer (CIO), who reports directly to the FDIC Chairman, has primary responsibility for IT governance, investments, program management, and information security. The FDIC's Chief Information Security Officer (CISO) reports directly to the CIO and is responsible for carrying out the CIO's responsibilities under FISMA—most notably the planning, development, and implementation of the FDIC's information security and privacy programs. The CIO and CISO coordinate closely with the Director of DIT, who is responsible for the day-to-day management of the FDIC's IT operations. The Director of DIT reports to the CIO. The individual serving as the FDIC's CIO resigned in 2015, and the FDIC currently has an Acting CIO. The FDIC has announced the appointment of a permanent CIO, who will begin serving in this role subsequent to the issuance of this report.

The FDIC's divisions and offices also play an important role in securing information and information systems. The FDIC designed its information security management program to ensure an enterprise-wide approach to information security. The FDIC has 12 ISMs representing the Division of Insurance and Research, DIT, Chief Information Officer Organization (CIOO), Division of Administration (DOA), Division of Finance, Division of Resolutions and Receiverships, Division of Depositor and Consumer Protection, Legal Division, Office of Complex Financial Institutions, Office of Inspector General (OIG), and Division of Risk Management Supervision. The ISMs provide a security focus within their respective divisions and offices and are tasked with working to educate employees and contractors who have access to corporate systems and data. Additionally, the ISMs assess the level of security in applications and service providers, assist in determining whether applications are considered major or minor, ensure that security requirements are addressed in new and enhanced systems, and promote compliance with FDIC security policies and procedures, among other security tasks.

The FDIC also has internal control liaisons that are responsible for, among other things, working with the ISMs to identify and ensure the implementation of security requirements in business process controls across the divisions and offices.

## Summary of Results

Overall, we found that, within the scope of work that we performed, the FDIC's information security program and practices are generally effective, except as described below. As part of our work, we noted several important improvements to the FDIC's information security program over the last year. Specifically, the FDIC:

- Enhanced its patch and vulnerability management program, which resulted in significant progress in addressing both the total number and the significance of outstanding vulnerabilities captured in POA&Ms. Contributing to these accomplishments was the creation of a Patch and Vulnerability Management Group (PVG), as well as subgroups to the PVG that specialize in various infrastructure platforms. These subgroups meet regularly to evaluate technical vulnerabilities in the IT environment and work to implement solutions to remediate those vulnerabilities, principally through vendor patches. These groups follow the FDIC's Patch Management Policy established in June 2014.

- Made progress in improving its process for managing known weaknesses through POA&Ms. Due in part to management's focus on open high-risk POA&Ms, the number of high-risk POA&Ms has decreased from 49 in September 2014 to 26 in August 2015.
- Improved its security metrics reporting, particularly to senior management, which has enhanced awareness and enabled management to take more proactive measures to improve the FDIC's overall information security posture.

(b)(5),(b)(7)(E) (b)(5),(b)(7)(E) Further, in March 2015, the FDIC revised its Circular [redacted] [redacted] to better align with NIST guidance. Among other things, the new policy places greater emphasis on the roles and responsibilities of the FDIC's divisions and offices to ensure that information security risks and controls are addressed throughout the life cycle of their information systems. In this regard, division and office ISMs play a critical role in addressing information security requirements and risks within the FDIC's business units. ISMs are often in the best position to identify and address information security risks that are specific to business processes and controls within their divisions and offices that might not otherwise come under the attention of ISPS or DIT staff.

As described later in our report, we identified several issues pertaining to the ISM role that warrant management's attention. Specifically:

- Although the duties and role of the ISMs have evolved since the ISM program was established, the FDIC has not recently completed a comprehensive assessment to determine whether the ISMs' current skills and resource allocations are appropriate to fulfill their assigned duties and to effectively manage information security risks within the FDIC's divisions and offices.
- Although ISPS communicates new security policy guidance and awareness training to ISMs at the monthly held ISM Committee meeting and invites the ISMs to attend the monthly held cyber security lunch-and- learn sessions where they can learn about industry best practices and awareness on security trends, the FDIC has not developed and mandated specific role-based training for the ISMs to ensure they fully understand their assigned duties and continue to maintain the skill sets needed to effectively fulfill their important role.
- The organizational structure in which the ISMs reside presents certain challenges in consistently measuring ISM performance and ensuing accountability.

In addition, we noted that ISMs have not always carried out their required duties. Among other things, we noted that:

- Outsourced information service provider assessments were often not performed,
- Access certifications were not performed in a timely manner, and
- Outsourced information service provider security documentation was not always adequately reviewed.

The FDIC should assess the skills, resource allocations, training, and oversight required for the ISM role and, based on the results of that assessment, address any identified gaps.

Our report describes other important security initiatives that the FDIC was working to implement, including a multi-year effort to identify, document, implement, and monitor secure baseline configurations for its information systems. While the initial implementation of such configurations takes time and the overall process will be a continuous one, we encourage management to place continued priority on this effort.

Although not considered a finding, we noted that the FDIC depends heavily on its IT infrastructure services contract (ISC) to support its IT operations and implement security controls. Contracts such as the ISC present certain risks, such as award protests, unsatisfactory performance, and metrics that do not effectively measure results against desired outcomes. The prior ISC contract vendor protested the results of the last competition, which delayed implementation of the contract. In addition, [redacted] (b)(4),(b)(5) [redacted] (b)(4),(b)(5) [redacted] (b)(4),(b)(5) FDIC officials informed us that they were aware of these risks and were working to mitigate them.

Our report includes additional findings in the areas of risk management, continuous monitoring management, identity and access management, and configuration management. We have prioritized our findings, with the highest-risk items listed first. We are providing a total of six recommendations to improve the FDIC's information security program and practices.

## AUDIT FINDINGS

### 1. The FDIC should assess the ISM role.

**Condition**

A. The original requirements for the ISM role were established 13 years ago. Since that time, information security requirements for federal agencies have grown considerably, and the threat environment is far more complex and sophisticated. The evolving nature of information security has resulted in a dramatic increase in the expectations for the FDIC's ISM role. For example, the 2014 revisions to the FDIC's ISM Guide describe a role that requires significant IT technical knowledge and information security risk management expertise. Some of the duties identified in the ISM Guide include:

- Developing and approving divisional security and privacy policies and procedures.
- Undertaking research so as to offer current and credible expertise on security and privacy issues.
- Performing day-to-day management of division IT project/initiative security/privacy portfolio.
- Serving as point of contact for divisional Computer Security Incident Response Team incidents and data breaches.

- Reviewing and commenting on draft directives dealing with corporate security and privacy matters.
- Leading their respective divisions in all phases of the Risk Management Framework, including:
  - Risk Assessment
  - POA&M Management
  - System Security Plan Development and Maintenance
  - Privacy Impact Assessments
  - Contingency Planning
  - Outsourced Information Service Provider Assessments

Although the duties required of the ISMs and their role has evolved over the past 13 years, the FDIC has not recently completed a comprehensive assessment to determine whether the ISMs' current skills and resource allocations are appropriate to fulfill the duties identified in the ISM Guide and to effectively manage information security risks within the FDIC's business divisions and offices.

B. Although ISPS communicates new security policy guidance and awareness training to ISMs at the monthly ISM Committee meetings and invites the ISMs to attend monthly cyber security lunch-and-learn sessions where they can learn about industry best practices and awareness of security trends, the FDIC has not developed and mandated specific role-based training for the ISMs to ensure that they fully understand their assigned duties and continue to maintain the skill sets needed to effectively fulfill their important role.

C. ISMs have not always carried out their duties in a timely manner. Specifically, as of August 31, 2015, (b)(5) the [redacted] reported that ISMs only completed required outsourced information service provider assessments for 47 of the 130 providers assigned to the two highest-risk categories. In addition, the (b)(5) [redacted] metrics on access certifications[3] reported that, as of August 24, 2015:

- 56 of the 116 completed access certifications were finished after their due date.
- 37 of the 81 planned access certifications were scheduled to begin on a date in the past.
- 7 of the 16 in-process access certifications were past their due date.

**Criteria**

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* states:

> *AT-3 ROLE-BASED SECURITY TRAINING*
>
> *Control: The organization provides role-based security training to personnel with assigned security roles and responsibilities:*
>
> *a. Before authorizing access to the information system or performing assigned duties;*

[3] Access certification refers to the process of validating a system's user base and the users' associated system access.

*b. When required by information system changes; and*

*c. [Assignment: organization-defined frequency] thereafter.*

*SA-9 EXTERNAL INFORMATION SYSTEM SERVICES*

*Control: The organization:*

*a. Requires that providers of external information system services comply with organizational information security requirements and employ [Assignment: organization-defined security controls] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;*

*b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and*

*c. Employs [Assignment: organization-defined processes, methods, and techniques] to monitor security control compliance by external service providers on an ongoing basis.*

*AC-2 ACCOUNT MANAGEMENT*

*Control: The organization:*

*j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency];*

**Cause**

The ISMs are located within divisions and offices throughout the FDIC. As a result, the Acting CIO does not have direct oversight of the ISMs. The organizational placement of the ISMs offers certain benefits, such as promoting the integration of information security into the FDIC's business processes; however, it also presents challenges, such as balancing competing priorities and ensuring consistent measurement of ISM performance and accountability.

In 2012, the FDIC Chairman established the Executive Management Committee (EMC) to assist the Chairman and Board of Directors in the day-to-day operational and strategic management of the FDIC. The EMC is responsible for identifying key operational and strategic priorities and overseeing timely coordination of issue follow-up. Thus, EMC can facilitate an assessment of the skill sets, resource allocations, role-based training, and oversight of the ISM program.

**Effect**

Absent a comprehensive assessment of the ISM role, the FDIC has reduced assurance that it can effectively address the risks associated with a rapidly changing threat environment. In addition, if ISMs do not complete the critical security requirements described above, the FDIC will be exposed to increased or unknown risks.

**Recommendations**

We recommend that the Acting CIO, in coordination with the EMC:

1. Assess the role of the ISMs in managing information security risks within the FDIC's divisions and offices. At a minimum, the assessment should include:
    - Performing a gap analysis of the ISMs' current skill sets and resources and the skill sets and resources necessary to ensure that ISMs successfully execute their duties, today and into the future.
    - Evaluating whether the current approach to providing training to the ISMs is adequate, or whether more formal role-based security training is warranted.
    - Determining whether the current lines of reporting and processes for measuring ISM performance are effective and ensure appropriate accountability.
2. Based on the results of the assessment in Recommendation 1, establish a plan to address any identified gaps.

**2. The FDIC had not fully implemented secure configuration baselines.**

In its report entitled *INFORMATION SECURITY, FDIC Made Progress in Securing Key Financial Systems, but Weaknesses Remain*, dated July 2014 (Government Accountability Office's (GAO) 2014 Security Report), GAO noted that the FDIC had not developed secure baseline configurations for administrators to use in consistently securing the FDIC's information systems. A baseline configuration is a set of specifications (e.g., configuration settings, software versions, patch levels, system documentation) for a system that has been formally approved and that can be changed only through change control processes. Without baseline configurations that are documented, implemented, and monitored, FDIC information systems may not be adequately protected. Accordingly, GAO recommended that the FDIC establish and implement baseline configurations for its information systems.

In response to the recommendation, the FDIC initiated a multi-year project to document, implement, and monitor against approved baseline configurations for its information systems, using NIST-approved checklists and the Center for Internet Security benchmarks as guides. Management has continued to make progress in this area and plans to substantially complete the project by the end of 2016.

As this finding is the result of a previously identified condition and has an outstanding recommendation, we are not providing any additional recommendations in this area.

**3. The FDIC production environment included vendor software that is no longer supported.**

**Condition**

(b)(5) As of August 28, 2015, the FDIC had [redacted] servers in the production environment, [redacted] (b)(5)
(b)(5) [redacted] The FDIC had identified this risk and has a plan in place to either upgrade or retire each of these servers.

**Criteria**

NIST SP 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, Section 3.5, *SDLC Phase: Disposal*, Subsection 3.5.1 states:

> *Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. When information systems are transferred, become obsolete, or are no longer usable, it is important to ensure that government resources and assets are protected.*

**Cause**

Management had initiated a project to decommission its [redacted] servers, with a planned completion date in advance of the vendor discontinuing support. However, this project was being managed under the ISC, the FDIC's primary infrastructure services support contract, [redacted] [redacted] [redacted] ultimately caused FDIC management to adjust its priorities, and as a result, the decommissioning of the servers was not completed on the original schedule.

(b)(5)
(b)(4),(b)(5)
(b)(4)
(b)(4),(b)(5)

**Effect**

Software vendors do not identify and provide security fixes for unsupported software. As a result, the FDIC is at increased risk of being exposed to security vulnerabilities for which there are not easily deployable solutions. This elevates the risk to the confidentiality, integrity, and availability of FDIC systems and data.

**Recommendation**

FDIC management already has a plan in place to address this risk. Therefore, we are not providing any additional recommendations in this area.

4. **The FDIC did not regularly track risks identified during assessments of outsourced information service providers.**

**Condition**

Management has implemented a formal process for assessing outsourced information service providers and uses the [redacted] to identify whether ISMs have completed their assessments; however, the FDIC does not have a standard mechanism in place [redacted] [redacted]

(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)

**Criteria**

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, states:

*RA-3 RISK ASSESSMENT*

*Control: The organization:*

*a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;*

*b. Documents risk assessment results in [Selection: security plan; risk assessment report; [Assignment: organization-defined document]];*

*c. Reviews risk assessment results [Assignment: organization-defined frequency];*

*d. Disseminates risk assessment results to [Assignment: organization-defined personnel or roles]; and*

*e. Updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.*

**Cause**

Management did not have a mechanism to formally communicate the above referenced types of risks within or outside of the divisions and offices.

**Effect**

(b)(5),(b)(7)(E) FDIC management does not have access to the risks identified through its outsourced information service provider assessments; [redacted]

(b)(5),(b)(7)(E) [redacted] The FDIC may, therefore, be exposing itself to risks that it would not normally accept.

**Recommendation**

We recommend that the Acting CIO:

3. Implement a process for capturing risks identified as part of the outsourced information service provider assessments and presenting these risks to management on a regular basis. This process should be integrated with the risk management processes already in place at the FDIC, such as the POA&M process.

**5. The FDIC had not fully implemented multi-factor authentication.**

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, recommends that agencies implement multi-factor authentication for network access to privileged (i.e., administrator) and non-privileged (i.e., user) accounts on moderate-impact information systems. In addition, in June 2015, the United States CIO instructed federal agencies to dramatically accelerate implementation of multi-factor authentication, especially for privileged users. According to the United States CIO, requiring the use of multi-factor authentication can significantly reduce the risk of adversaries penetrating federal networks and systems.

The FDIC has required multi-factor authentication for remote network access for many years. In 2012, the OIG recommended that the FDIC implement multi-factor authentication for privileged network users, and in 2013, it recommended that the FDIC develop plans for requiring multi-factor authentication for general network users. The FDIC has implemented multi-factor authentication for privileged network users; however, it recently identified security weaknesses in the solution and is currently addressing these weaknesses. The FDIC recently selected a solution to implement multi-factor authentication for general network users and will begin work on this project in 2015, with continued implementation during 2016. Continued management attention and strong governance over this initiative is warranted to ensure its success.

As this finding is the result of a previously identified condition and has outstanding recommendations, we are not providing any additional recommendations in this area.

(b)(5),(b)(7)(E) **6. [redacted] did not log events.**

(b)(5),(b)(7)(E) GAO's 2014 Security Report noted that the FDIC had not yet resolved three issues related to auditing and monitoring controls, [redacted]

(b)(5),(b)(7)(E) [redacted]

As this finding is the result of a previously identified condition and has outstanding recommendations, we are not providing any additional recommendations in this area.

**7. The FDIC did not complete timely information service provider assessments.**

**Condition**

The FDIC did not perform assessments of outsourced information service providers as required by its *Outsourced Information Service Provider Assessment Methodology*. We reviewed the [redacted] (b)(5)
(b)(5) [redacted] and noted that:

- For Trust Level 3 outsourced service providers (those with the highest risk), the ISMs did not complete 6 out of 21 assessments, or 29 percent of the assessments.
- For Trust Level 2 outsourced service providers, the ISMs did not complete 77 out of 109 assessments, or 71 percent of the assessments.

**Criteria**

The FDIC's *Outsourced Information Service Provider Assessment Methodology* states:

> *The FDIC is responsible for managing risks to organizational information and protecting the confidentiality, integrity, and availability of the sensitive data that is processed by Outsourced*

*Information Service Providers. To satisfy this responsibility, the FDIC has established the Outsourced Information Service Provider Assessment Methodology.*

*The Outsourced Information Service Provider Assessment Methodology outlined in this document is to be used by all Divisions and Offices for all outsourced information service providers that do business with the FDIC. Outsourced Information Service Provider artifacts must be collected on a yearly basis because these artifacts form the basis of creating the yearly Security Synopsis.*

**Cause**

The underlying causes for the lack of timely completion of information service provider assessments require additional analysis; however, a contributing cause is the absence of an effective process to evaluate and ensure that FDIC personnel perform information service provider assessments in a timely manner.

**Effect**

Recent highly-publicized data breaches at the Office of Personnel Management highlight the impact that can occur when security risks associated with outsourced information service providers are not effectively addressed. The lack of timely assessments of the FDIC's information service providers presents the FDIC with increased risk of unmitigated vulnerabilities.

**Recommendation**

We recommend that the Acting CIO:

4. Assess the ISM *Outsourced Information Service Provider Assessment Methodology* processes supporting information service provider assessments to determine and implement any needed improvements to ensure timely completion of assessments.

**8. The FDIC did not perform timely access certifications for its information systems.**

**Condition**

(b)(5)
(b)(5),(b)(7)(E)
(b)(5),(b)(7)(E)

The [redacted] provides an overview of the status of access certifications managed by the [redacted] [redacted] metrics on access certifications reported that, as of August 24, 2015:

- 56 of the 116 completed access certifications were finished after their due date.
- 37 of the 81 planned access certifications were scheduled to begin on a date in the past.
- 7 of the 16 in-process access certifications were past their due date.

**Criteria**

FDIC Circular 1360.15, *Access Control for Information Technology Resources*, states:

*Periodic reviews of access settings shall be conducted to ensure that appropriate controls remain consistent with existing authorizations and current business needs.*

**Cause**

Although ISMs share responsibility for ensuring that access certifications are performed in a timely manner, the final responsibility for completing access certifications ultimately rests with the System Owners in the various divisions. Division and office management can monitor completion of the access certifications through the Security and Privacy Dashboard. The FDIC does not fully understand the underlying causes for late and overdue certifications; however, a contributing cause [redacted] (b)(5)

(b)(5)

**Effect**

The access certification process is a key control for helping to ensure that only authorized users have access to FDIC systems and data, and that the level of access granted is appropriate. When the access certification process is not completed, there is an increased risk that access will not be removed timely once no longer needed and, therefore, an increased risk to the confidentiality, integrity, and availability of FDIC systems and data.

**Recommendation**

We recommend that the Acting CIO:

5. Assess the certification processes to determine and implement any needed improvements to ensure timely completion of access certifications.

**9. The FDIC did not properly manage user IDs and passwords for an outsourced information service.**

**Condition**

(b)(5),(b)(7)(E) [redacted]

**Criteria**

(b)(5),(b)(7)(E) FDIC Circular [redacted] states:

- *Users shall never give permission to another person to use their personal password, except as authorized* [redacted] *by the Director, Division of Information Technology (DIT).* (b)(5),(b)(7)(E) (b)(5),(b)(7)(E)

[redacted]

- *If an application/system cannot accommodate this requirement, it shall be configured to require the strongest level of password complexity possible within its configuration limitations.*
- *Passwords must be changed after 90 days using the password expiration facilities. Passwords can be changed in less than 90 days, but shall not be changed by the user more frequently than once per day.*

**Cause**

The FDIC did not address the password account requirements identified in FDIC Circular [redacted] when designing its business procedures for accessing information in [redacted]

(b)(5),(b)(7)(E)

(b)(4),(b)(5),(b)(7)(E)

**Effect**

(b)(4),(b)(5),(b)(7)(E)

Weaknesses in the [redacted] access controls increase the risk that sensitive information, including personally identifiable information, could be compromised, resulting in an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or public embarrassment for the FDIC.

**Recommendation**

We recommend that the Director, DOA:

6. Take appropriate steps to address the risks associated with the use of user IDs and passwords to access sensitive information in [redacted]

(b)(4),(b)(5),(b)(7)(E)

## STATUS OF PRIOR-YEAR FISMA RECOMMENDATIONS

(b)(5),(b)(7)(E)

The following table summarizes the status of previously unaddressed recommendations from the OIG's 2013 and 2014 security evaluation reports required by FISMA.

| Recommendation(s) | Status |
|---|---|
| **2013 FISMA Recommendation 5**<br>Update Circular [redacted] (b)(5),(b)(7)(E) | Closed. |
| **2013 FISMA Recommendation 10**<br>Address potential gaps that may exist between the 12-hour timeframe required to restore mission-essential functions following an emergency and the 72-hour recovery time objective for restoring mission-critical applications. | Open – FDIC plans to complete corrective action by 12/31/2016. |
| **2014 FISMA Recommendation 1**<br>Adopt new or modified security controls, as appropriate, consistent with NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4. | Open – FDIC plans to complete corrective action by 7/16/2016. |
| **2014 FISMA Recommendation 2**<br>Develop and approve a written ISCM strategy consistent with OMB and NIST guidance. | Closed. |
| (b)(5),(b)(7)(E)<br>**2014 FISMA Recommendation 3**<br>Develop and approve written procedures to govern the testing of operating system patches (including documentation requirements) for the [redacted] (b)(5),(b)(7)(E) | Closed. |
| **2014 FISMA Recommendation 4**<br>Review and enhance (where appropriate) existing procedures designed to ensure that security vulnerabilities identified during technical security assessments are recorded in OpenFISMA in a timely manner. | Closed. |
| **2014 FISMA Recommendation 5**<br>Conduct an internal assessment of the effectiveness of the FDIC's POA&M process after a reasonable period of time is allowed for the implementation of planned and ongoing improvement initiatives. | Closed. |

## APPENDIX I – LIST OF ACRONYMS

| Acronym | Description |
|---|---|
| CIO | Chief Information Officer |
| CIOO | CIO Organization |
| CISO | Chief Information Security Officer |
| DHS | Department of Homeland Security |
| DIT | Division of Information Technology |
| DOA | Division of Administration |
| EMC | Executive Management Committee |
| FISMA | Federal Information Security Modernization Act |
| GAO | Government Accountability Office |
| IG | Inspector General |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| P.L. | Public Law |
| SP | Special Publication |

# *Part II*

# *Corporation Comments and OIG Evaluation*

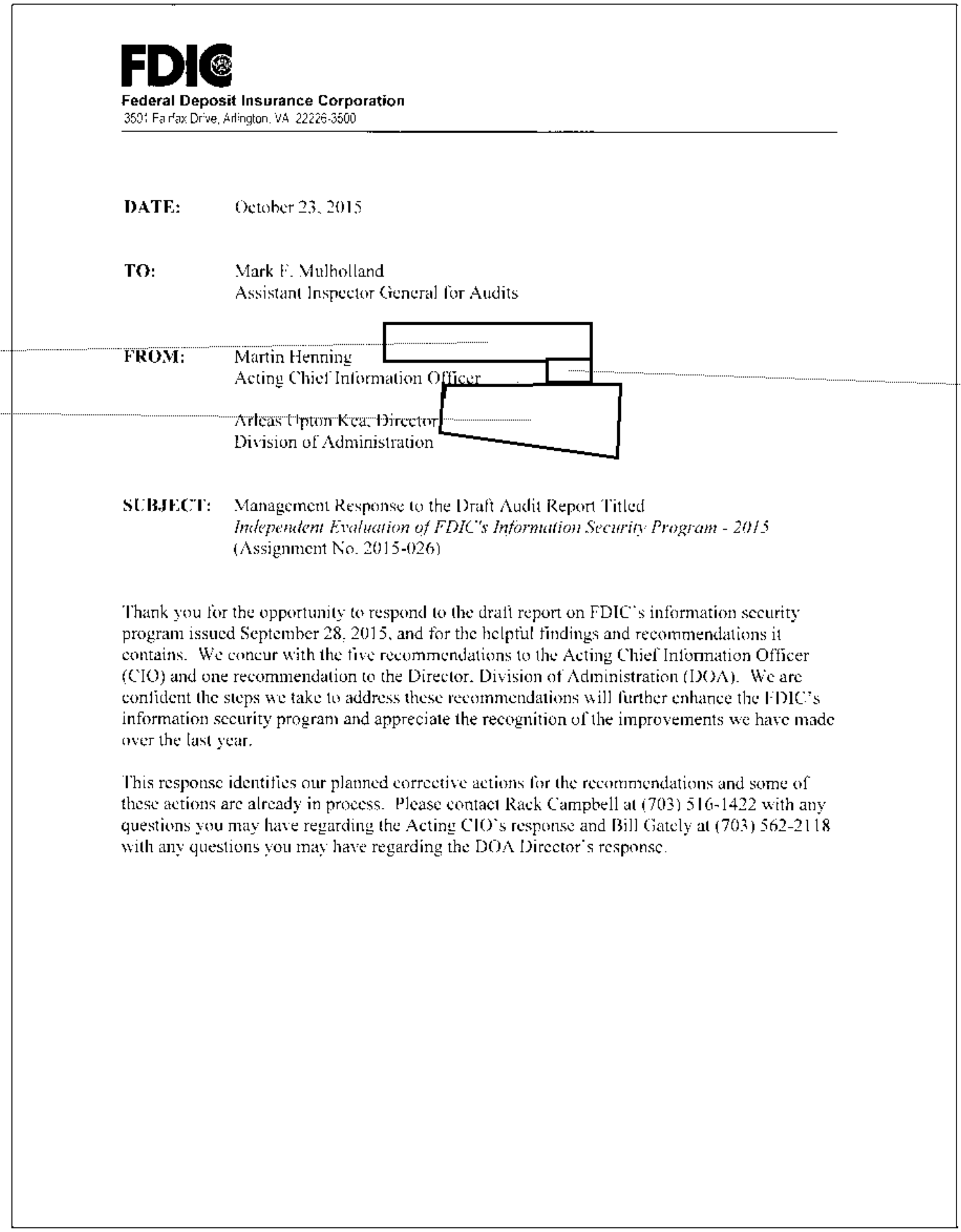
## Corporation Comments and OIG Evaluation

Subsequent to the issuance of C&C's draft report, FDIC officials provided additional information for C&C's consideration, and the firm revised its report to reflect this information, as appropriate. The FDIC's Acting CIO and Director, DOA, provided a joint written response, dated October 23, 2015, to a draft of C&C's report. The response is presented in its entirety beginning on page II-2. In the response, FDIC management concurred with all six of the report's recommendations.

A summary of the response and expected completion dates for each recommendation begins on page II-6. The planned and completed actions are responsive for all six recommendations, and all of the recommendations are resolved.

With respect to Recommendations 4 and 5, we plan to assess the FDIC's implementation of any plan of actions to address needed improvements as part of our 2016 security evaluation work required by FISMA.

## Corporation Comments



**FDIC**

**Federal Deposit Insurance Corporation**
3501 Fairfax Drive, Arlington, VA 22226-3500

**DATE:** October 23, 2015

**TO:** Mark F. Mulholland
Assistant Inspector General for Audits

(b)(6)

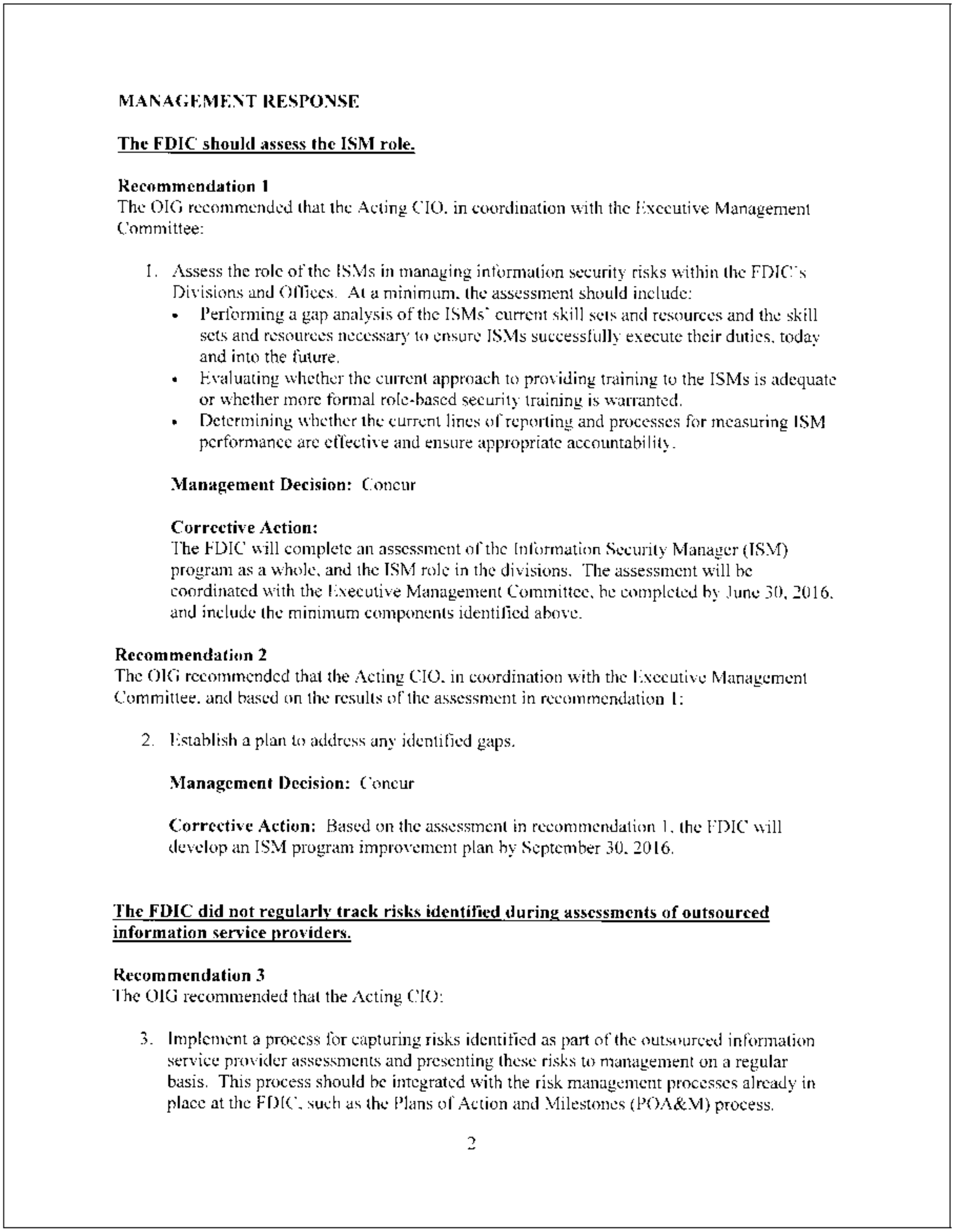
**FROM:** Martin Henning
Acting Chief Information Officer (b)(6)

(b)(6) Arleas Upton Kea, Director
Division of Administration

**SUBJECT:** Management Response to the Draft Audit Report Titled
*Independent Evaluation of FDIC's Information Security Program - 2015*
(Assignment No. 2015-026)

Thank you for the opportunity to respond to the draft report on FDIC's information security program issued September 28, 2015, and for the helpful findings and recommendations it contains. We concur with the five recommendations to the Acting Chief Information Officer (CIO) and one recommendation to the Director, Division of Administration (DOA). We are confident the steps we take to address these recommendations will further enhance the FDIC's information security program and appreciate the recognition of the improvements we have made over the last year.

This response identifies our planned corrective actions for the recommendations and some of these actions are already in process. Please contact Rack Campbell at (703) 516-1422 with any questions you may have regarding the Acting CIO's response and Bill Gately at (703) 562-2118 with any questions you may have regarding the DOA Director's response.



**MANAGEMENT RESPONSE**

**<u>The FDIC should assess the ISM role.</u>**

**Recommendation 1**
The OIG recommended that the Acting CIO, in coordination with the Executive Management Committee:

1. Assess the role of the ISMs in managing information security risks within the FDIC's Divisions and Offices. At a minimum, the assessment should include:
   - Performing a gap analysis of the ISMs' current skill sets and resources and the skill sets and resources necessary to ensure ISMs successfully execute their duties, today and into the future.
   - Evaluating whether the current approach to providing training to the ISMs is adequate or whether more formal role-based security training is warranted.
   - Determining whether the current lines of reporting and processes for measuring ISM performance are effective and ensure appropriate accountability.

   **Management Decision:** Concur

   **Corrective Action:**
   The FDIC will complete an assessment of the Information Security Manager (ISM) program as a whole, and the ISM role in the divisions. The assessment will be coordinated with the Executive Management Committee, be completed by June 30, 2016, and include the minimum components identified above.

**Recommendation 2**
The OIG recommended that the Acting CIO, in coordination with the Executive Management Committee, and based on the results of the assessment in recommendation 1:

2. Establish a plan to address any identified gaps.

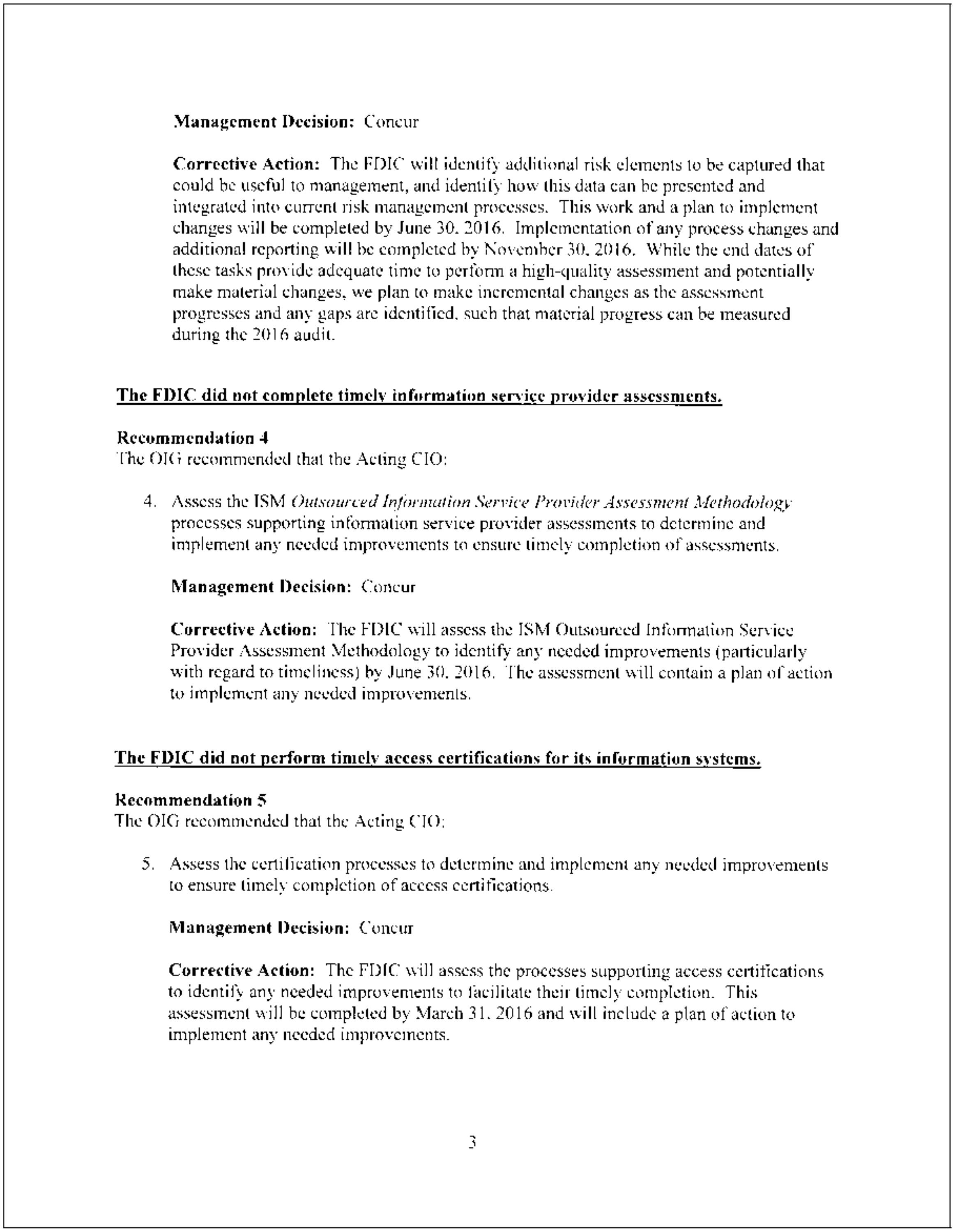
   **Management Decision:** Concur

   **Corrective Action:** Based on the assessment in recommendation 1, the FDIC will develop an ISM program improvement plan by September 30, 2016.

**<u>The FDIC did not regularly track risks identified during assessments of outsourced information service providers.</u>**

**Recommendation 3**
The OIG recommended that the Acting CIO:

3. Implement a process for capturing risks identified as part of the outsourced information service provider assessments and presenting these risks to management on a regular basis. This process should be integrated with the risk management processes already in place at the FDIC, such as the Plans of Action and Milestones (POA&M) process.



**Management Decision:** Concur

**Corrective Action:** The FDIC will identify additional risk elements to be captured that could be useful to management, and identify how this data can be presented and integrated into current risk management processes. This work and a plan to implement changes will be completed by June 30, 2016. Implementation of any process changes and additional reporting will be completed by November 30, 2016. While the end dates of these tasks provide adequate time to perform a high-quality assessment and potentially make material changes, we plan to make incremental changes as the assessment progresses and any gaps are identified, such that material progress can be measured during the 2016 audit.

**<u>The FDIC did not complete timely information service provider assessments.</u>**

**Recommendation 4**
The OIG recommended that the Acting CIO:

4. Assess the ISM *Outsourced Information Service Provider Assessment Methodology* processes supporting information service provider assessments to determine and implement any needed improvements to ensure timely completion of assessments.

   **Management Decision:** Concur

   **Corrective Action:** The FDIC will assess the ISM Outsourced Information Service Provider Assessment Methodology to identify any needed improvements (particularly with regard to timeliness) by June 30, 2016. The assessment will contain a plan of action to implement any needed improvements.

**<u>The FDIC did not perform timely access certifications for its information systems.</u>**

**Recommendation 5**
The OIG recommended that the Acting CIO:

5. Assess the certification processes to determine and implement any needed improvements to ensure timely completion of access certifications.

   **Management Decision:** Concur

   **Corrective Action:** The FDIC will assess the processes supporting access certifications to identify any needed improvements to facilitate their timely completion. This assessment will be completed by March 31, 2016 and will include a plan of action to implement any needed improvements.

**The FDIC did not properly manage User IDs and passwords for an outsourced information service.**

**Recommendation 6**
The OIG recommended that the Director, DOA:

6. Take appropriate steps to address the risks associated with the use of User IDs and passwords to access sensitive information in [redacted]

(b)(4),(b)(5),(b)(7)(E)

**Management Decision:** Concur

(b)(4),(b)(5),(b)(7)(E)

[redacted]

cc: James H. Angel. Jr., Deputy Director, DOF, Corporate Management Control
Daniel H. Bendler, Assistant Director, DOA, Management Services Branch
Christopher J. Farrow, CISO, Information Security & Privacy
Russell G. Pittman, Director, DIT
John S. Kidd, Deputy Director, DIT, Infrastructure Services Branch
Steven P. Anderson, Deputy Director, DIT, Business Administration Branch
Rack D. Campbell, Supervisory IT Specialist, DIT, Audit and Internal Control
William J. Gately, Jr., Management Analyst, DOA, Management Services Branch

## Summary of the Corporation's Corrective Actions

This table presents corrective actions taken or planned by the Corporation in response to the recommendations in the report and the status of the recommendations as of the date of report issuance.

| Rec. No. | Corrective Action: Taken or Planned | Expected Completion Date | Monetary Benefits | Resolved:[a] Yes or No | Open or Closed[b] |
|---|---|---|---|---|---|
| 1 | The FDIC will complete an assessment of the ISM program as a whole, and the ISM role in the divisions. The assessment will be coordinated with the EMC and include the minimum components identified in the recommendation. | 6/30/2016 | $0 | Yes | Open |
| 2 | Based on the results of the assessment in Recommendation 1, the FDIC will develop an ISM program improvement plan. | 9/30/2016 | $0 | Yes | Open |
| 3 | The FDIC will identify additional risk elements that could be useful to management, identify how this data can be presented and integrated into current risk management processes, and implement any needed process changes and additional reporting. | 11/30/2016 | $0 | Yes | Open |
| 4 | The FDIC will assess the *Outsourced Information Service Provider Assessment Methodology* to identify any needed improvements (particularly with regard to timeliness) and develop a plan of action to implement those improvements. | 6/30/2016 | $0 | Yes | Open |
| 5 | The FDIC will assess the processes supporting access certifications to identify any needed improvements to facilitate their timely completion and develop a plan of action to implement those improvements. | 3/31/2016 | $0 | Yes | Open |
| 6 | (b)(4),(b)(5),(b)(7)(E)<br>[redacted] | 12/31/2015 | $0 | Yes | Open |

## Summary of the Corporation's Corrective Actions

(b)(4),(b)(5),(b)(7)(E)

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |

[a] Resolved – (1) Management concurs with the recommendation, and the planned, ongoing, and completed corrective action is consistent with the recommendation.

(2) Management does not concur with the recommendation, but alternative action meets the intent of the recommendation.

(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Recommendations will be closed when (a) Corporate Management Control notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, when the OIG confirms that corrective actions have been completed and are responsive.