Office of Inspector General

January 2007
Report No. 07-003

The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005

AUDIT REPORT

Office of Audits

OIG

Office of Audits

OIG

Report No. 07-003
January 2007

The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005

Background and Purpose of Audit

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to audit the FDIC's compliance with section 522 of the Consolidated Appropriations Act, 2005 (Division H, The Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005) (section 522). Section 522 requires, among other things, that agencies establish and implement comprehensive privacy and data protection procedures and have an independent third-party review performed of their privacy programs and practices.

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships, the FDIC creates and acquires a significant amount of information in an identifiable form (IIF). Such IIF includes names, addresses, Social Security numbers, phone numbers, dates of birth, and credit report information. Much of the information managed by the FDIC falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure.

The objective of the audit was to (1) evaluate the FDIC's use of IIF and the FDIC's privacy and data protection procedures and (2) recommend strategies and specific steps to improve the FDIC's privacy and data protection management practices.

To view the full report, go to: www.fdicig.gov/2007reports.asp

Results of Audit

The FDIC has established a corporate-wide privacy program to protect the IIF it manages from unauthorized disclosure and ensure its appropriate use consistent with section 522. Of particular note, the FDIC has appointed a Chief Privacy Officer (CPO) with overall responsibility for the FDIC's privacy program, issued or drafted policies and procedures for safeguarding IIF, and posted a privacy statement on the FDIC's public Web site. Additionally, the FDIC has performed privacy impact assessments (PIA) on its systems identified as containing IIF, completed required Privacy Act-related reviews, and implemented mandatory Web-based privacy awareness training for its employees and contractors. Further, the FDIC was working to complete a number of key initiatives to strengthen its privacy program policies, procedures, and practices and ensure compliance with federal privacy-related statutes, policies, and guidelines.

Consistent with the intent of section 522, our report identifies areas of the FDIC's privacy program warranting continued management attention and recommends strategies and specific steps that management should take to ensure adequate protection of its IIF. Specifically, the FDIC can enhance its privacy program by integrating its key ongoing and planned program control activities into a formal documented plan. In addition, (a) physical security of IIF in hardcopy format needed improvement; (b) PIAs posted on the FDIC's public Web site did not always contain sufficient descriptions of the FDIC's collection or use of IIF; and (c) the FDIC's System Development Life Cycle (SDLC) processes did not address all relevant aspects of privacy, including the role of privacy officials.

Recommendations and Management Response

KPMG recommended that the CPO:

- enhance the FDIC's privacy program by integrating key ongoing and planned program control activities into a formal documented plan;
- implement additional measures to ensure that IIF is properly secured;
- place additional emphasis on employee and contractor awareness to physically safeguard IIF in their custody;
- ensure that PIAs posted on the FDIC's public Web site adequately describe the FDIC's collection and use of IIF; and
- enhance the FDIC's SDLC processes to fully address privacy.

The FDIC agreed with the recommendations and is taking responsive actions.

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: January 10, 2007

MEMORANDUM TO: Michael E. Bartell
Chief Privacy Officer,
Chief Information Officer, and
Director, Division of Information Technology

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005*
(Report No. 07-003)

Attached is a copy of the subject report prepared by KPMG LLP under contract with the Office of Inspector General. Please refer to the Executive Summary for the overall results of the audit. The firm's report is presented as Part I of this document.

A summary and evaluation of your response, the response in its entirety, and the status of the report's recommendations are contained in Part II of this document. Your comments on a draft of this report were responsive to the report's recommendations. We consider the recommendations to be resolved, but they will remain open until we have determined that agreed-to corrective actions have been completed and are effective.

If you have any questions concerning the report, please contact Mark F. Mulholland, Director, Systems Management and Security Audits, at (703) 562-6316. We appreciate the courtesies extended to the audit staff during the assignment.

Attachment

cc: Rack D. Campbell, DIT
James H. Angel, Jr., OERM

Table of Contents

Part I

Report by KPMG LLP

The FDIC's Compliance With Section 522 of the Consolidated Appropriations Act, 2005 (Report No. 07-003)

Prepared for the Federal Deposit Insurance Corporation Office of the Inspector General

FINAL REPORT

Prepared by:

KPMG LLP
Advisory Services, Federal Practice
2001 M Street, NW
Washington, DC 20036
(202) 533-3000

TABLE OF CONTENTS

ACRONYMS

AICPA	American Institute of Certified Public Accountants
ASA	Application Security Assessment
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
CPO	Chief Privacy Officer
DSC	Division of Supervision and Consumer Protection
DIT	Division of Information Technology
DRR	Division of Resolutions and Receiverships
FDIC	Federal Deposit Insurance Corporation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Auditing Standards
GPRA	Government Performance and Results Act
IIF	Information in an Identifiable Form
ISM	Information Security Manager
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OERM	Office of Enterprise Risk Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RUP®	Rational Unified Process
SDLC	Systems Development Life Cycle
SP	Special Publication
SSN	Social Security Number

INTRODUCTION

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct a performance audit of the FDIC's compliance with section 522 of the Consolidated Appropriations Act, 2005 (section 522).[1] Section 522 requires, among other things, that agencies establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form (IIF)[2] relating to agency employees and the public. Section 522 also requires agency Inspectors General to contract with an independent third party to review and report on their agencies' privacy programs and practices. The FDIC has determined that section 522 applies to the Corporation.

The objective of the audit was to (1) evaluate the FDIC's use of IIF and the FDIC's privacy and data protection procedures and (2) recommend strategies and specific steps to improve the FDIC's privacy and data protection management practices. As part of the audit, we followed up on privacy-related issues contained in two previously-issued OIG reports.[3] We conducted our performance audit in accordance with generally accepted government auditing standards (GAGAS) issued 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 objectives. Appendix I describes our objective, scope, and methodology; Appendix II contains brief descriptions of key privacy-related laws, policies, and guidelines and their applicability to the FDIC; Appendix III describes the criteria used to assign risk ratings to the detailed findings contained in this report; Appendix IV provides an overview of the FDIC's privacy program initiatives; and Appendix V presents concepts from the global privacy framework developed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA).

---

[1] Section 522 is found in Division H of the Consolidated Appropriations Act, 2005, entitled the *Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005*. For convenience, we are using "Consolidated Appropriations Act, 2005" in the title of this audit and elsewhere in this report.

[2] The Office of Management and Budget's (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* defines IIF as information in an information system or an on-line collection that directly identifies an individual (e.g., name, address, Social Security number (SSN), or other identifying code, telephone number, e-mail address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements. Our report uses the term IIF when referring to personally identifiable information (PII) to be consistent with section 522. See Appendix II for further information about this definition.

[3] *The FDIC's Efforts to Comply with OMB Memorandum M-06-16, Protection of Sensitive Agency Information* (Report No. 06-020), dated September 2006; and *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 06-018), dated September 2006.

BACKGROUND

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships, the FDIC creates and acquires a significant amount of IIF. Such IIF includes names, addresses, SSNs, phone numbers, dates of birth, and credit reports related to FDIC employees and contractors and depositors and borrowers at FDIC-insured financial institutions. Much of the information managed by the FDIC and its contractors falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure. These statutes and regulations include section 522; the Privacy Act of 1974; section 208 of the E-Government Act of 2002; and Parts 309, *Disclosure of Information*, and 310, *Privacy Act Regulations*, of the FDIC's Rules and Regulations. Further, OMB has issued a number of privacy-related policies and guidelines to federal departments and agencies aimed at protecting IIF.[4] In addition, the FDIC has developed internal policies and procedures to safeguard the IIF the Corporation manages.

Section 522 Requirements

Enacted in December 2004, section 522 directs agencies, including the FDIC, to implement a number of measures to protect IIF. Such measures include:

- Appointing a Chief Privacy Officer (CPO) to assume primary responsibility for agency privacy and data protection policy.
- Establishing and implementing comprehensive privacy and data protection procedures governing the collection, use, sharing, disclosure, transfer, storage, and security of IIF relating to agency employees and the public. Such procedures are to be consistent with legal and regulatory guidance, including OMB regulations; the Privacy Act of 1974; and section 208 of the E-Government Act of 2002.
- Preparing a written report, signed by the CPO, that provides a benchmark for the agency's privacy program and describes the agency's use of IIF, along with its privacy and data protection policies and procedures. The report is to be recorded with the agency Inspector General.

Section 522 also requires agencies to have an independent, third-party review of the agency's use of IIF to (a) determine the accuracy of the agency's description of IIF use; (b) determine the effectiveness of privacy and data-protection procedures; (c) ensure compliance with the stated privacy and data protection policies of the agency and applicable laws and regulations; and (d) ensure that all technologies used to collect, use, store, and disclose IIF allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program. In general, the review is required to be performed at least every 2 years by a third party with expertise in privacy under the cognizance of the agency Inspector General. Upon completion of the review, the agency Inspector General must submit to the agency head a detailed report that includes recommendations for improvements and enhancements to the agency's management

[4] See Appendix II for pertinent OMB privacy-related policies and guidelines.

of IIF and its privacy and data protection procedures and strategies to improve privacy and data protection management.

The FDIC's Privacy Program

The FDIC has established a corporate-wide privacy program consisting of various policies and procedures for managing and protecting its IIF. These include a corporate policy directive governing the collection, maintenance, use, and/or dissemination of records subject to the Privacy Act of 1974; procedures for identifying IIF contained in applications;[5] and procedures for completing privacy impact assessments (PIA)[6] of systems containing IIF. In March 2005, the FDIC appointed a senior official, the Chief Information Officer (CIO), as the FDIC's CPO with overall responsibility for the Corporation's privacy program. The FDIC also designated a Privacy Program Manager to support the CPO in developing and implementing corporate privacy requirements. In October 2005, the FDIC implemented mandatory annual privacy awareness training for its employees and contractors that includes guidance on protecting IIF and coverage of privacy laws, regulations, and policies. In addition, the FDIC implemented a privacy program Web site to promote awareness of privacy requirements, policies, and practices and installed shredding bins in its facilities to securely dispose of sensitive information, including IIF. Further, as required by section 522, the CPO provided a written report to the OIG on September 15, 2005, describing the FDIC's use of IIF, along with the FDIC's privacy and data protection policies and procedures.

In addition, the FDIC is in the process of implementing a number of initiatives aimed at strengthening its privacy program policies, procedures, and practices and ensuring compliance with privacy-related laws and regulations. Of particular note, the FDIC is working to:

- Identify all IIF maintained by the FDIC's divisions and offices, regardless of where the information is stored (e.g., in network applications; freestanding, limited use, or user-created applications; databases; and network shares). Based on the results of this effort, the Division of Information Technology (DIT) will determine whether additional safeguards are necessary to protect the information and whether public disclosure regarding its collection and use is adequate.
- Identify all FDIC contractors having custody of privacy-related information, and verify whether appropriate safeguards are in place.

[5] The FDIC uses the Application Security Assessment (ASA) document to assess the security of its applications. The ASA includes questions for identifying IIF.

[6] A PIA is an analysis of how information is handled to: (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating IIF, and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. A PIA is required by the E-Government Act of 2002 (as implemented by OMB Memorandum M-03-22) to ensure privacy protections, and the requirements of the Privacy Act of 1974 are considered when developing or procuring new or modified information technology (IT) that contains IIF.

- Issue several draft corporate-policy directives related to privacy that include guidance for the secure storage, transmission, remote access, dissemination/transport, and disposal of sensitive information, including IIF.
- Confirm that adequate privacy-related controls are in place for systems identified as containing IIF by completing the security checklist provided by the National Institute of Standards and Technology (NIST).[7]
- Consolidate the annual privacy awareness and security awareness training modules into a single program to achieve efficiencies.
- Research methods to ensure that technologies used to collect, use, store, and disclose IIF allow for continuous auditing of compliance with stated privacy policies and practices as required by section 522.

Appendix IV contains a detailed description of the FDIC's key privacy-related initiatives and their status as of October 2006.

Protecting IIF is a Government-wide Challenge

Safeguarding IIF from unauthorized disclosure has been, and continues to be, of significant concern to both the public and the Congress. Common threats associated with the compromise of IIF include identity theft and consumer fraud. In response to highly publicized breaches of sensitive personal information at federal agencies, the Committee on Government Reform of the U.S. House of Representatives (the Committee) requested 19 federal departments and agencies to provide the Committee with information about incidents involving the loss or compromise of sensitive personal information (i.e., IIF) held by the agency or its contractors.[8] The Committee issued a report, dated October 13, 2006, based on the information it received, stating that all 19 departments and agencies had experienced at least 1 loss of IIF since January 1, 2003. The report noted that the majority of these losses arose from physical thefts of portable computers, drives, and disks, or unauthorized use of data by agency employees. The Committee's report concluded that, taken as a whole, the agencies had identified hundreds of instances of data breaches involving IIF and that each incident had affected from one individual to as many as millions of individuals. The Committee's report emphasizes the criticality of having an effective and comprehensive privacy program.

[7] OMB's June 23, 2006 Memorandum M-06-16, *Protection of Sensitive Agency Information*, recommends that agencies complete the NIST checklist. The memorandum also recommends encryption, authentication, and logging controls for sensitive information.

[8] The Committee issued the request, dated July 10, 2006, to all Cabinet-level agencies, the Office of Personnel Management, and the Social Security Administration.

RESULTS OF AUDIT

The FDIC has established a corporate-wide privacy program to protect the IIF it manages from unauthorized disclosure and ensure its appropriate use consistent with section 522. Of particular note, the FDIC has appointed a CPO with overall responsibility for the FDIC's privacy program, issued or drafted corporate policies and procedures for safeguarding IIF, and posted a privacy statement on the FDIC's public Web site. Additionally, the FDIC has performed PIAs on its systems identified as containing IIF, completed required Privacy Act-related reviews,[9] and implemented mandatory Web-based privacy awareness training for its employees and contractors. Further, as described in the Background section of this report, the FDIC was working to complete a number of key initiatives to strengthen its privacy program policies, procedures, and practices and ensure compliance with federal privacy-related statutes, policies, and guidelines.

Consistent with the intent of section 522, our report identifies areas of the FDIC's privacy program warranting continued management attention and recommends strategies and specific steps that management should take to ensure adequate protection of its IIF. Specifically, the FDIC can strengthen its privacy program by integrating its key ongoing and planned program control activities into a formal documented plan. In addition, the FDIC needs to (a) implement additional control measures to ensure the physical security of its IIF in hardcopy format, (b) ensure that PIAs posted on the FDIC's public Web-site adequately describe the FDIC's collection and use of IIF, and (c) fully address privacy-related considerations in its System Development Life Cycle (SDLC)[10] processes. Such actions will help ensure that IIF managed by the FDIC is adequately protected and that the FDIC's privacy practices are consistent with section 522 and related statutes, policies, and procedures.

STRATEGY FOR ENHANCING CURRENT PRIVACY PROGRAM EFFORTS

Section 522 requires that independent third-party reviews of agency privacy programs recommend strategies and specific steps to improve the agencies' privacy and data protection management. As part of this review, we have identified one such strategy that the FDIC can implement to strengthen its privacy program management. Although not mandated by statute or regulation, the FDIC can enhance its privacy program by documenting a formal, comprehensive plan that integrates the Corporation's privacy program goals and objectives, performance measures, organization and relationship of key initiatives, training and awareness strategy, and methods for reporting.

The FDIC established a corporate-wide privacy program and was working diligently to address current and emerging privacy-related requirements. As discussed in the Background section of this report, the FDIC was working on initiatives to identify all FDIC- and

---

[9] OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*, requires agencies to perform various reviews of compliance with certain provisions of the Privacy Act of 1974. See Appendix II for details.

[10] The SDLC is a process for developing information systems through several phases, each comprised of multiple steps.

contractor-maintained IIF throughout the Corporation, develop new privacy policy directives, enhance the Corporation's privacy awareness training, and ensure adequate controls are in place to protect privacy data in applications. The FDIC was also performing a number of ongoing privacy activities, such as conducting and reporting PIAs, providing awareness training to employees and contractor personnel, and addressing new OMB privacy requirements. FDIC privacy officials (i.e., the CPO and Privacy Program Manager) were coordinating these initiatives and activities with various internal organizations and corporate officials, such as the FDIC's CIO Council, Legal Division, and systems owners throughout the Corporation. Also, privacy officials were preparing various privacy-related reports and briefings for FDIC management, OMB, and the Congress.[11]

Although the FDIC developed the *IT Strategic Plan 2004 – 2007* and the *Information Security Strategic Plan 2006 – 2007* to help manage its IT and security program activities, these plans do not address privacy activities. The FDIC could enhance its privacy program management by integrating its key ongoing and planned program control activities into a formal, comprehensive documented plan. Such a plan would promote integration of the FDIC's:[12]

- Privacy program goals and objectives.
- Performance measures to assess the extent to which the FDIC is achieving its privacy program goals and objectives.[13]
- Privacy program roles and responsibilities.
- Organization and relationship of key FDIC initiatives that support its privacy program goals and objectives.
- Training and awareness to foster an improved control environment and a corporate culture that emphasizes the importance of the protection of IIF. Although the FDIC's efforts to identify its IIF are not yet complete, we observed that additional training and awareness on what IIF is and where it can reside (e.g., in standalone systems, databases, and network shares) would be helpful to system owners responsible for identifying IIF.
- Methods for reporting privacy program activities and remedial actions.

[11] Such reporting includes, but is not limited to, the FDIC's annual privacy reporting required by the Federal Information Security Management Act of 2002 (FISMA), biennial reporting required by section 522, and periodic status reporting to the FDIC Operating Committee, OIG, and others.

[12] The FDIC could address some of these items (in whole or in part) in other corporate plans, such as its *Corporate Annual Performance Plan*, *IT Strategic Plan*, and *Information Security Strategic Plan*. Additionally, at the time of our audit, the FDIC was considering the inclusion of two measures in its 2007 Corporate Performance Objectives to enhance its privacy program.

[13] Developing strategic plans, setting performance goals, and reporting results is a fundamental tenet of the Government Performance and Results Act of 1993 (GPRA). GPRA requires agencies, including the FDIC, to measure how program activities accomplish agency strategic goals and objectives.

In May 2006, the AICPA/CICA published a global privacy framework entitled, *Generally Accepted Privacy Principles* (the Framework).[14] The principles contained in the Framework are based on current international privacy regulatory requirements and industry-accepted practices and are designed to be applied to any organization's privacy program. Although the FDIC is not required to adhere to the Framework, it does contain certain business practices that can benefit the FDIC's privacy program.

Figure 1: AICPA/CICA Privacy Framework

Source: AICPA/CICA *Generally Accepted Privacy Principles.*

Figure 1 identifies five primary activities associated with managing a privacy program as defined by the Framework. The first activity, *Strategizing*, involves the development of an "overall master plan" to ensure that the organization's efforts are headed in a common direction. The plan defines, among other things, the strategic direction of the organization's privacy program, the organization's long-term goals and major issues for becoming privacy-compliant, processes for achieving goals and milestones, and a mechanism for communicating critical privacy program information. The remaining four activities in Figure 1 flow from *Strategizing*.

As previously discussed, the FDIC has established a corporate-wide privacy program. Implementing such a program is a major, multi-year effort requiring sustained coordination among divisions and offices throughout the Corporation. Documenting a comprehensive plan that integrates key aspects of the Corporation's privacy program as described above will facilitate the proactive identification of potential program gaps, weaknesses, and redundancies. Such a plan could also further facilitate integration of ongoing and planned privacy program activities, help address current and emerging privacy requirements, and promote sound program governance.

Recommendation

We recommend that the FDIC CPO:

1. Enhance the FDIC's privacy program by integrating key ongoing and planned program control activities into a formal documented plan.

[14] Appendix V contains additional information on the Framework. See also http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/.

DETAILED AUDIT RESULTS

PHYSICAL SECURITY OF HARDCOPY IIF

Risk Rating: Moderate

Condition

The FDIC has taken a number of steps to ensure the physical security of hardcopy IIF and IIF stored on portable storage media such as compact disks, flash drives, and microfiche. Such measures included placing lockable file cabinets and secure storage facilities in FDIC buildings, providing employees and contractors with guidance on how to protect sensitive information through security awareness training, and issuing advisories to employees and contractor personnel through global e-mail messages and the FDIC's privacy Web site. However, additional measures are needed. On October 17, 2006, KPMG and OIG staff performed walkthroughs of selected floors in FDIC buildings located in Washington, D.C.; Arlington, Virginia; and Dallas, Texas, and found 15 separate instances in which significant amounts of IIF stored in hardcopy format and on portable storage media had not been properly secured.[15] Unsecured IIF included employee names, addresses, and SSNs; borrower SSNs, borrower loan numbers, court records, and death certificates; and one instance of an individual's name and credit card number. Generally, the IIF was stored in unlocked file cabinets, unsecured file rooms, and boxes placed in hallways and other building common areas.

Although physical access controls such as security guards and identification badges were in place to restrict building entry to only authorized personnel and visitors, further restrictions to ensure the principle of least privilege[16] were not in place. We immediately notified the FDIC's Computer Security Incident Response Team of the unsecured IIF that we identified during our walkthroughs and were advised that prompt corrective action was taken to secure the information.

Cause

Although the FDIC had taken some steps to promote awareness of the need to secure IIF, the Corporation was not monitoring employee and contractor compliance with physical IIF security requirements. Such monitoring could include, for example, performing periodic walkthroughs of FDIC facilities to determine whether IIF is properly secured. Employees and contractor personnel are less likely to leave IIF unsecured if compliance controls are in place. Additionally, the FDIC had not implemented procedures for visibly marking all documents containing IIF to heighten awareness of the need to protect such information.

---

[15] The OIG reported weaknesses in the FDIC's physical security of sensitive information, including IIF, in its September 2006 reports entitled, *Independent Evaluation of the FDIC's Information Security Program-2006* (Report No. 06-022) and *DRR's Protection of Bank Employee and Customer Personally Identifiable Information* (Report No. 06-017).

[16] Least privilege refers to the concept of restricting access to information resources to the minimum level necessary to perform a specific function (e.g., job duty).

Further, the FDIC had drafted, but not yet issued, a corporate directive defining guidelines for the protection of sensitive electronic and hardcopy information (including IIF), such as storing documents containing sensitive information in locked file drawers when not in use, and never leaving portable IT equipment unattended.

Additional emphasis on employee awareness is warranted until such time as FDIC divisions and offices determine that IIF is being consistently secured throughout the Corporation. Such emphasis could be in the form of advisories in the annual privacy awareness training, reminders from division and office information security managers, and awareness briefings in division and office conferences. Additional considerations may include the implementation of a clean-desk policy and the labeling of sensitive documents and files, including those containing IIF.

Criteria

The Privacy Act of 1974 states that agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. The FDIC CPO issued a global e-mail message on July 26, 2006 directing all employees and contractor personnel to "secure hard copies of PII [i.e., IIF] until they are properly disposed…safeguard hard copies in your work areas, and shred them when they are not longer needed." Subsequent global e-mail messages from the CPO reiterated the responsibilities of employees and contractor personnel to secure IIF.

The FDIC's security awareness training instructs employees and contractor personnel to protect sensitive data in both electronic and hardcopy formats from disclosure to unauthorized individuals or groups. The awareness training states, "Leaving diskettes and CD's lying around is tantamount to leaving your computer turned on without a password-protected screen saver. They are easily taken and used by anyone with access to a computer. If you have important and/or confidential information on a diskette or CD, take care to store it properly in a locked drawer." Further, the FDIC's internal Web site, *Protecting Sensitive Information*, states, "whenever sensitive information is stored on portable media or printed out in hard copy, such information should be kept secure and in a locked file cabinet when appropriate."

Effect

Absent appropriate measures to ensure that IIF is properly secured in FDIC facilities, the FDIC is at increased risk of a potential unauthorized disclosure or compromise of IIF. Such a compromise could result in individual identity theft and unnecessary costs to the Corporation resulting from remediation efforts (such as notifications to affected individuals and potential credit monitoring services). In addition, unauthorized access to, and use of, IIF poses considerable risk to the FDIC's reputation, as well as to the individuals whose data is not protected.

Recommendations

We recommend the FDIC CPO:

2. Implement additional control measures to ensure IIF is properly secured. Such measures could include marking documents containing IIF and performing periodic, unannounced walkthroughs of FDIC facilities and reporting the results to appropriate management officials.

3. Place additional emphasis on employee and contractor awareness to physically safeguard IIF in their custody as previously discussed in this report.

PUBLIC DISCLOSURE OF IIF USAGE

Risk Rating: Moderate

Condition

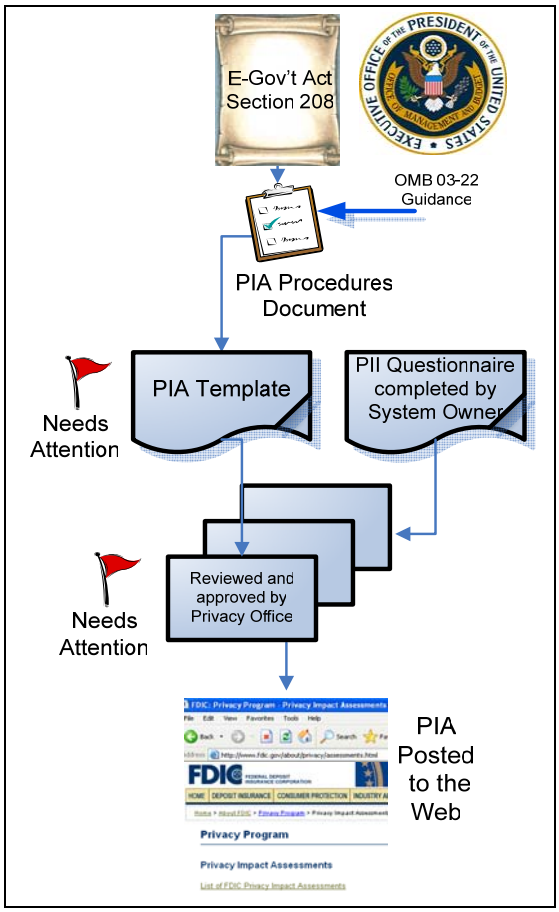
The FDIC has established a formal process for conducting PIAs[17] of its applications and systems that contain IIF and posted PIAs on its public Web site. However, PIAs posted on the FDIC's public Web site did not always contain sufficient information regarding the collection or use of IIF as described in OMB policy and section 208 of the E-Government Act of 2002. We judgmentally selected 15 of the 43 PIAs posted on the FDIC's public Web site as of October 27, 2006 and found that 6 of the 15 PIAs did not disclose all types of IIF collected and/or stored by the application.[18] In addition, 3 of the 15 PIAs that we reviewed did not adequately describe how or why the IIF contained in the application was being used. PIAs for these three applications provided a general description of the application rather than a description of the intended use of each type of IIF collected or stored.

[17] The purpose of a PIA is to analyze and publicly disclose how personal information is collected, used, stored, shared, and protected by government agencies.

[18] Of the six PIAs, two did not disclose any types of IIF collected by the application. The remaining four PIAs did not disclose at least one type of IIF (e.g., date of birth, home telephone number, or bank account number) collected by the application.

Cause

Figure 2: The FDIC's PIA Process
Source: KPMG Analysis.



As reflected in Figure 2, the FDIC's PIA process consists of three key documents: (1) a formal PIA Procedures document containing detailed instructions and examples to assist division and office personnel in conducting PIAs, (2) a PII Questionnaire to aid FDIC personnel in identifying IIF, and (3) a PIA Template to document the results of PIA work and later post to the FDIC's public Web site. Because questions in the PIA Template are more general than the PIA Procedures document and PII Questionnaire, the PIA Template did not always ensure that individuals responsible for completing PIAs provided specific information regarding IIF collection and use. As a result, PIAs posted on the FDIC's public Web site did not always include prescribed privacy-related information that detailed the type of information collected, the reason(s) why the information was collected, and the intended use of the information.

On October 31, 2006, a DIT official informed us that efforts were underway to combine the PIA Template and PII Questionnaire into a single document. Such streamlining should improve the efficiency of the FDIC's PIA process and provide additional assurance that PIAs posted on the FDIC's public Web site are consistent with privacy-related requirements. The FDIC should also consider additional reviews of PIA content by appropriate officials prior to public posting of PIAs to ensure they sufficiently address IIF collection and use.

Criteria

In general, Section 208 of the E-Government Act of 2002 requires agencies to conduct PIAs of all information systems containing IIF and make the completed PIAs available to the public. The Act requires that published PIAs describe, among other things, what information is to be collected, why the information is being collected, and the agency's intended use of the information. OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act*, provides details on the required content of PIAs. Among other things, the OMB memorandum states that PIAs must analyze and describe the type of information to be collected (e.g., nature and source); why the information is being collected (e.g., to determine eligibility); and the intended use of the information (e.g., to verify existing data).

Effect

PIAs are intended to promote the public trust through increased transparency and assurances that personal information is protected. Absent full disclosure of this information, the Corporation's use of IIF may not be clearly understood by the public through reviews of published PIAs.

Recommendations

We recommend that the FDIC CPO:

4. Review all PIAs posted on the FDIC's public Web site to determine whether they disclose all types of IIF used by the application and sufficiently describe the FDIC's use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

5. Enhance current processes for preparing and publicly posting PIAs to ensure that new PIAs adequately describe the FDIC's collection and use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

PRIVACY CONSIDERATIONS IN THE SDLC

Risk Rating: Low

Condition

The FDIC adopted the Rational Unified Process (RUP®)[19] SDLC methodology in 2004 and tailored the RUP® to meet the specific needs of the Corporation. Of particular note, the FDIC tailored the RUP® to address information security requirements applicable to each phase of the SDLC and describe the roles of key corporate committees and personnel involved in the SDLC.[20] One such requirement includes the completion of an ASA that includes steps for identifying IIF in systems under development.[21] However, the FDIC's SDLC processes do not fully address privacy considerations. Such privacy considerations include, for example, the role of privacy officials, such as the CPO and Privacy Program Manager, in the development, maintenance, and disposal of information systems. Privacy considerations also include ensuring that IIF protection needs are addressed throughout a system's life cycle.[22] Addressing such privacy considerations during the SDLC will

[19] RUP® is an iterative and risk-based methodology for developing information systems. RUP® is a registered trademark of Rational Software Corporation, a wholly-owned subsidiary of the International Business Machines (IBM®) Corporation.

[20] Such committees and personnel include the Capital Investment Review Committee, CIO Council, Enterprise Architecture Board, Program Management Office, and DIT Information Security Staff.

[21] In the event the ASA identifies the presence of IIF, completion of a PIA for the system is required.

[22] Such protection needs are dynamic because privacy requirements and risks change over time. Examples include encrypting IIF stored in databases, suppressing IIF data when printed on paper, and generating audit trails of IIF data downloads.

provide the FDIC with greater assurance that privacy requirements are identified and addressed in an efficient and timely manner during systems development and implementation.

Cause

A number of new privacy-related requirements have been imposed on federal agencies in recent years in response to reports of security breaches involving IIF. Such privacy requirements include security control and reporting provisions contained in section 522 and privacy safeguards described in OMB policy memoranda. As discussed in the Background section of this report, the FDIC was working to implement a number of key initiatives aimed at addressing new and emerging privacy requirements. Because the FDIC's privacy program is relatively new and evolving, the Corporation had not yet fully addressed privacy considerations in its SDLC processes.

We spoke with DIT personnel and FDIC privacy officials about the importance of privacy considerations in the SDLC. A DIT official informed us that FDIC system developers use an electronic requirements template as part of the FDIC's SDLC processes. The template contains requirements, such as NIST-recommended security controls and standards for complying with section 508 of the Rehabilitation Act,[23] that developers consider when developing systems. The DIT official indicated that privacy considerations could be added to the requirements template to ensure that privacy is adequately considered in the SDLC process. We agree that modifying the requirements template would be a prudent step toward addressing privacy in the FDIC's SDLC processes.

Criteria

The SDLC is a key control for ensuring that security and privacy are integrated into the life-cycle planning and management of information systems. NIST Special Publication (SP) 800-64, *Security Considerations in the Information Systems Development Life Cycle*, describes key roles and responsibilities associated with information systems development, including the role of the privacy officer. According to the publication, privacy officers and other officials play a critical role in ensuring that systems meet existing privacy policies regarding protection, dissemination (information sharing and exchange), and information disclosure. In addition, NIST SP 800-64 states that the process of identifying functional requirements should include an analysis of relevant laws and regulations, including the Privacy Act of 1974. Although the FDIC is not required to comply with NIST SP 800-64, it contains prudent business practices related to privacy that the FDIC should voluntarily adopt.

[23] Section 508 requires federal agencies that develop, procure, maintain, or use electronic and IT systems to ensure that federal employees and members of the public with disabilities have access to and use of information and data, comparable to that of the employees and members of the public without disabilities, unless it is an undue burden to do so. The FDIC has determined that it is not legally bound to follow section 508 but does so as a matter of policy.

Effect

According to NIST SP 800-64, information security is most effective when it is integrated into the SDLC methodology from its inception. Industry research has shown that addressing IT requirements early in a system's life-cycle development is less costly than if the requirements are addressed in later life-cycle phases. Ensuring that privacy considerations are fully addressed in the FDIC's SDLC processes will promote a defined and repeatable approach for incorporating privacy controls into new systems and provide FDIC management greater assurance that privacy requirements are identified and addressed in an efficient and effective manner. Such efforts will also help ensure that the confidentiality and integrity of IIF are maintained.

Recommendation

We recommend that the FDIC CPO:

6. Enhance the FDIC's SDLC processes to fully address privacy considerations.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to (1) evaluate the FDIC's use of IIF and the FDIC's privacy and data protection procedures and (2) recommend strategies and specific steps to improve the FDIC's privacy and data protection management practices. KPMG conducted its performance audit in accordance with GAGAS issued by the Comptroller General of the United States. Those standards require that we (i.e., KPMG) plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish the audit objective, KPMG leveraged prior audit work as described in the OIG's September 2006 reports entitled, *The FDIC's Efforts to Comply with OMB Memorandum M-06-16, Protection of Sensitive Agency Information* (Report No. 06-020); and *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 06-018). Also, KPMG interviewed key FDIC privacy, security, and program office officials who had responsibility for implementing the FDIC's privacy program and complying with the requirements described in section 522 and OMB Memorandum M-06-16. KPMG reviewed relevant security- and privacy-related policies, procedures, and guidelines that address the control measures described in section 522. In addition, KPMG reviewed the FDIC's established procedures and guidance for performing PIAs and sampled a selection of publicly-posted PIAs for compliance with section 208 of the E-Government Act of 2002. Further, KPMG selected a sample of information systems to assess the progress of the FDIC's efforts to identify applications containing IIF. KPMG interviewed the business owners of the selected information systems to become familiar with processes used to identify IIF. KPMG also reviewed the FDIC's Web sites and Intranet and leveraged scans of the FDIC's network performed as part of the FISMA audit efforts to identify the presence of IIF. To evaluate physical protections over IIF, KPMG and the OIG performed walkthroughs of three FDIC facilities in Washington, D.C.; Arlington, Virginia; and Dallas, Texas.

KPMG did not evaluate program performance measures. In addition, KPMG did not perform procedures to determine the validity or reliability of computer-based data because such procedures were not critical to satisfying the audit's objectives. KPMG conducted alternative procedures to determine the presence of IIF data and the status of privacy initiatives, such as interviews of application owners. In addition, KPMG's assessments of the FDIC's management controls and compliance with laws and regulations were limited to those related to privacy, particularly those dealing with agency privacy-management requirements. Further, KPMG did not design tests to detect fraud, waste, abuse, and mismanagement. However, throughout the audit, KPMG was sensitive to the potential for fraud, waste, abuse, and mismanagement. KPMG conducted its work at the FDIC's offices in Arlington, Virginia; and Washington, D.C., during October 2006. The FDIC OIG performed certain other audit procedures at the FDIC's offices in Dallas, Texas.

LAWS, STANDARDS, POLICIES, AND GUIDELINES PROTECTING PRIVACY-RELATED AND SENSITIVE INFORMATION

In addition to requirements in section 522 of the Consolidated Appropriations Act, 2005, a number of federal statutes, standards, policies, and guidelines are aimed at protecting IIF from unauthorized use, access, disclosure, or sharing and associated information systems from unauthorized access, modification, disruption, or destruction. Brief descriptions of key privacy-related statutes, policies, and guidelines and their applicability to the FDIC follow.

- **The Privacy Act of 1974** imposes various requirements for federal agencies whenever they collect, create, maintain, and distribute records (as defined in the Act, and regardless of whether they are in hardcopy or electronic format) that can be retrieved by the name of an individual or other identifier. One such requirement is to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained. As a federal agency, the FDIC is subject to the requirements of the Act. The Act can be located at http://www.usdoj.gov/oip/privstat.htm.

- **The E-Government Act of 2002, section 208,** requires agencies to (1) conduct PIAs of information systems and collections and, in general, make PIAs publicly available; (2) post privacy policies on agency Web sites used by the public; (3) translate privacy policies into a machine-readable format; and (4) report annually to the OMB on compliance with section 208. The FDIC has determined that it is subject to the requirements of this provision. The Act can be located at http://www.cio.gov/archive/e_gov_act_2002.pdf.

- **Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems***, describes standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of impact levels. This publication establishes security categorization standards for information and information systems based on the potential impact on an organization should certain events occur that jeopardize the information and information systems needed by the organization to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. By its terms, this publication is not legally binding on the FDIC, but the FDIC intends to follow its principles. The publication can be located at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

- **NIST SP 800-64, *Security Considerations in the Information Systems Development Life Cycle,*** provides a framework for incorporating security into all phases of the information SDLC process, from initiation to disposal. Included within the framework are requirements to consider privacy protection measures in accordance with relevant privacy-related federal guidance. The provisions of this publication are non-mandatory.

The publication can be located at http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf.

- **NIST SP 800-30, *Risk Management Guide for Information Technology Systems,*** provides a foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The publication also provides information on the selection of cost-effective security controls. Such controls can be used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. The publication can be located at http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

- **OMB Circular No. A-130, *Management of Federal Information Resources,* Appendix I, *Federal Agency Responsibilities for Maintaining Records about Individuals***, describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974. The FDIC has determined that OMB Circular No. A-130, Appendix I, applies to the Corporation. Subsequent OMB policy provides additional information regarding agency responsibilities for designating a senior agency official for privacy, conducting PIAs, developing privacy policies for Web sites, providing privacy education to employees and contractor personnel, and reporting privacy activities. The circular can be located at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

- **OMB Memorandum M-03-18, *Implementation for the E-Government Act of 2002***, provides agencies information on implementing the E-Government Act of 2002. The guidance (1) outlines federal agency requirements related to the E-Government Act of 2002; (2) explains the information agencies are expected to provide under the E-Government Act of 2002 to support ongoing initiatives and new activities, including reports; (3) explains how the E-Government Act of 2002 authorizes certain ongoing government-wide initiatives; and (4) explains how the E-Government Act of 2002 fits within existing IT policy, such as policies included in OMB Circulars A-11, *Preparation, Submission, and Execution of the Budget;* and A-130, *Management of Federal Information Resources*. According to the FDIC, to the extent that the provisions of OMB Memorandum M-03-18 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/m03-18.pdf.

- **OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,*** provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, particularly section 208. The guidance directs agencies, including the FDIC, to conduct reviews of how IT is used to collect information about individuals or when agencies develop or buy new IT systems to handle collections of IIF, the definition of which appears in footnote 2 of this report. OMB's definition implements the E-Government Act's definition of "identifiable form," namely, "any representation of information that permits the identity of an individual to whom the information applies to be inferred by either direct or indirect means." Section 522 incorporates this statutory definition. We believe that

using OMB's definition of IIF is appropriate in connection with section 522 because, according to section 522, its definition of "identifiable form" is consistent with the E-Government Act's definition of the term. This memorandum replaces OMB memoranda 99-18, *Privacy Policies on Federal Web Sites;* and 00-13, *Privacy Policies and Data Collection on Federal Web Sites*. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/m03-22.html.

- **OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy,*** requests that agencies designate a senior official for privacy. The FDIC complied with the memorandum by designating the CIO as the senior agency official. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf.

- **OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information***, describes responsibilities and policy for appropriately safeguarding sensitive PII and for training employees on their responsibilities in this area. OMB requires the senior agency official for privacy to conduct a review of policies and processes and take corrective action as appropriate to ensure adequate safeguards exist to prevent misuse or authorized access to PII. Any weaknesses are to be identified in a security plan of action and milestones required by FISMA. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-15 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf.

- **OMB Memorandum M-06-16, *Protection of Sensitive Agency Information***, includes a checklist for agency use for protecting PII that is remotely accessed or transported outside the agency. The checklist is based on NIST SPs 800-53, *Recommended Security Controls for Federal Information Systems;* and 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft). In addition, M-06-16 recommends the encryption of all data on mobile computers/devices that carry sensitive data, two-factor authentication for remote access, "time-out" functions for remote access and mobile devices, and the logging of all computer-readable data extracts from databases containing sensitive information. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-16 are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf.

- **OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments***, provides updated guidance on the reporting of security incidents involving PII and explains the requirements agencies will need to address regarding security and privacy in fiscal year 2008 budget submissions for IT. This guidance requires all agencies to report all suspected or confirmed breaches involving PII in an electronic or physical form within 1 hour of discovering the incident to U.S. Center Emergency Readiness Team, a federal incident response center located within the Department of Homeland Security. According to the FDIC, to the extent that the provisions of OMB Memorandum M-06-19 are legally binding on the FDIC, the FDIC

has taken steps to implement those provisions or has otherwise taken them into account. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf.

- **OMB Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,*** directs senior agency officials for privacy to answer a series of questions about their agency's privacy programs. These questions are based, in part, on agency implementation of the privacy provisions of the E-Government Act of 2002. In addition, the memorandum requires the agency officials to report on the results of privacy program reviews and identify physical or electronic incidents involving the loss of or unauthorized access to IIF. The memorandum also requests that agency IGs provide information about their agency's privacy program and related activities, as appropriate, and provide a list of any systems not included in the agency's inventory of major information systems. The FDIC's practice is to comply with OMB's reporting guidance. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf.

- **OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notification,*** recommends agencies establish a core management group responsible for responding to the loss of personal information that poses the subsequent risk of identity theft. The group is to plan for contingencies in the event of a breach, evaluate the risk of identity theft associated with realized data losses, and take appropriate actions based on the determined risk. The FDIC considers this memorandum a background discussion paper that provides recommendations for agencies for planning and responding to data breaches. The memorandum can be located at http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf.

- **FDIC Rules and Regulations.** Part 309, *Disclosure of Information*, sets forth the basic policies of the FDIC regarding the information it maintains and the procedures for obtaining access to such information. Part 310, *Privacy Act Regulations*, establishes regulations implementing the Privacy Act of 1974 by delineating the procedures that an individual must follow in exercising his or her access or amendment rights under the Privacy Act of 1974 to records maintained by the Corporation in systems of record. FDIC Rules and Regulations Part 309 can be located at http://www.fdic.gov/regulations/laws/rules/2000-3800.html. FDIC Rules and Regulations Part 310 can be located at http://www.fdic.gov/regulations/laws/rules/2000-3900.html.

- **FDIC Circular 1031.1, *Administration of the Privacy Act,*** establishes requirements for the collection, maintenance, use, and dissemination of records subject to the Privacy Act of 1974.

- **Division of Information Technology IT Policy Memorandum, *Cookies in Internet Products,*** establishes the policy and standard for the use of cookies in Internet, FDICnet, and extranet-type products developed or deployed by the FDIC.

RISK RATINGS

Based on our experience and knowledge of industry practices, we assessed the risk associated with each control weakness described in the report and assigned a risk rating of High, Moderate, or Low. We based each risk rating on an analysis of our underlying audit work, and each rating required professional judgment as to the relative risk and significance of control strengths and weaknesses. We based our assessments of risk, in part, on concepts defined in FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, and risk definitions contained in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

A **High Risk** rating indicates a condition that could directly result in unauthorized access to internal networks or systems, a severe loss of data integrity, or a severe loss of system availability. NIST SP 800-30 describes a risk as "High" if "there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible."

A **Moderate Risk** rating is a condition that alone would not result in unauthorized access but does provide significant capability or information that could be directly used in conjunction with other information or tools to gain unauthorized access to internal systems. In regard to the security control objectives of integrity and availability, a moderate risk condition represents a condition that may have a serious adverse affect on data integrity or a serious loss of system availability. NIST SP 800-30 states that if a moderate risk is observed, then corrective actions are needed, and a plan must be developed to incorporate these actions within a reasonable period of time.

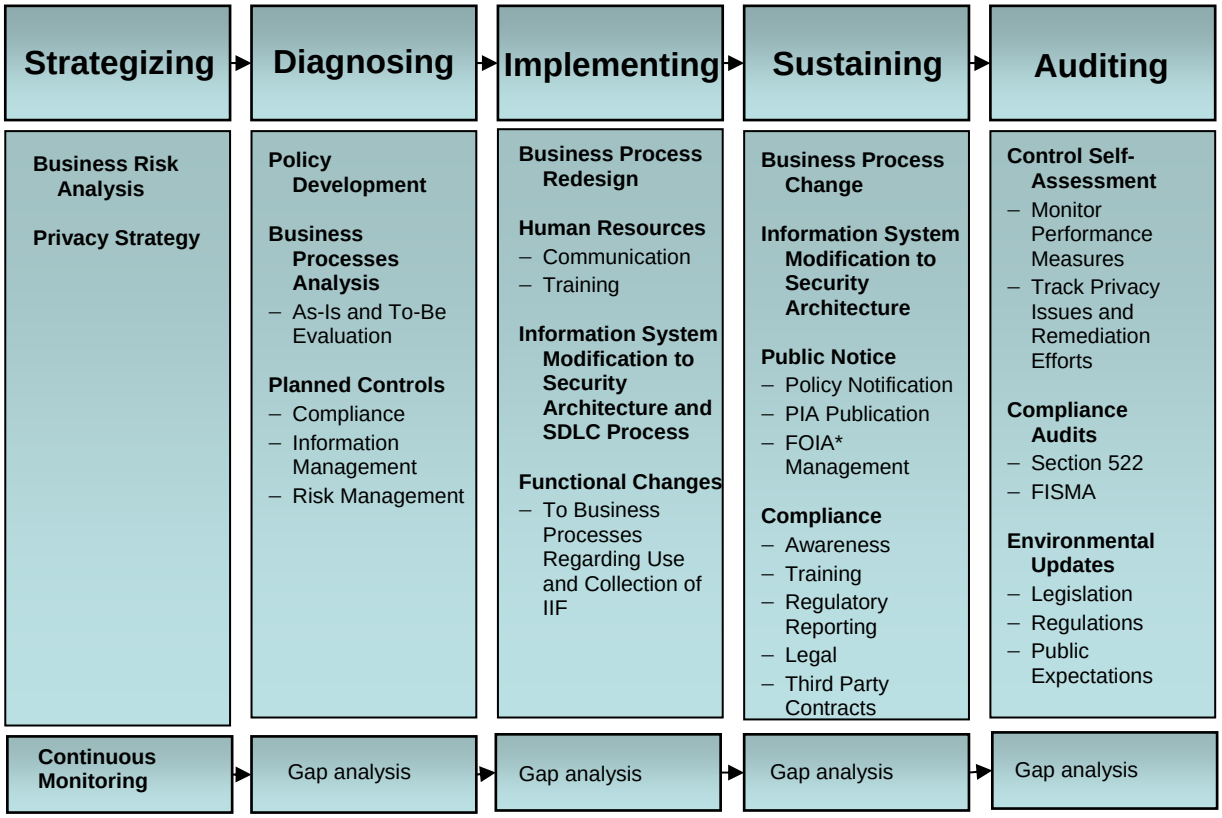
A **Low Risk** rating is a condition that does not directly lead to compromise of internal systems but demonstrates an incomplete approach to security. In regard to the security control objectives of integrity and availability, a low-risk condition represents a condition that may have a limited adverse affect on data integrity or a limited loss of system availability. NIST SP 800-30 characterizes a risk as "Low" if, "The system's Designated Approving Authority must determine whether corrective actions are still required or decide to accept the risk."

FDIC PRIVACY PROGRAM INITIATIVES

Privacy Area	Initiative	Status of Initiative as of October 20, 2006
Privacy Governance/ Policy	1. Increase privacy program staffing. 2. Develop a corporate-wide policy to address the protection of sensitive agency information, including IIF, and recent OMB requirements. 3. Research options to implement continuous monitoring of technologies used to collect, store, process, and disseminate IIF.	1. Ongoing. 2. A corporate-wide policy to address the requirements of the protection of sensitive information has been drafted but not yet issued. Interim policy in the form of global e-mails and divisional guidance has been communicated. 3. A group has been formed to research options to allow for continuous monitoring. Software solutions are under evaluation.
Privacy Web site	Develop and update a Web site devoted to privacy issues.	A Privacy Program Web site is established and is periodically updated (www.fdic.gov/about/privacy).
Privacy Training	1. Combine the security awareness and privacy awareness modules. 2. Develop classroom privacy training**.**	1. Storyboards (i.e., outlines) for combining the modules have been developed and are currently under review. Completion of work is planned for March 2007. 2. Coordination is planned with the Corporate University regarding classroom privacy training.
Privacy Awareness	Update the FDIC's incident reporting and response procedures to reflect the 1-hour reporting requirement contained in OMB Memorandum M-06-19.	Incident reporting procedures have been updated to reflect the 1-hour reporting requirement.
Privacy Impact Assessments	A PIA will be prepared for each information system containing personal information (i.e., IIF).	As of October 3, 2006, 43 PIAs had been performed for the 46 systems identified as containing IIF and posted on the Privacy Web site. As discussed in the report, work is ongoing to identify all IIF maintained throughout the Corporation.
Privacy Reporting	1. FISMA Privacy Reporting. 2. Section 522 Privacy Reporting. 3. Monthly privacy program status reports.	1. The 2006 FISMA privacy report was issued on September 28, 2006. 2. The memorandum on the FDIC's privacy program was sent to the Deputy Inspector General on September 15, 2005; a report to the Congress is planned by the end of 2006. 3. Monthly privacy program status reports have been produced since July 2006.
Compliance with OMB Memorandum M-06-16	1. Encrypt sensitive data stored on mobile computing devices. 2. Provide tokens to state bank examiners for remote authentication. 3. Finalize policy and implement software solution to log data extracts of sensitive data.	1. Current testing and implementation schedules suggest that data on laptops will be encrypted by December 2006. Encryption of external storage media and Blackberry devices will follow in February 2007. 2. Legal issues associated with providing tokens to state bank examiners are under review. Target completion is March 2007. 3. Draft policy is under review, and the FDIC is evaluating several software solutions to log data extracts.

AICPA/CICA PRIVACY FRAMEWORK CONCEPTS

The figure below highlights privacy program management concepts contained in the AICPA/CICA's global privacy framework entitled, *Generally Accepted Privacy Principles*. Other privacy frameworks exist; the AICPA/CICA's Framework is just one example for consideration.



Note: KPMG has expanded upon the AICPA/CICA'S Framework to incorporate applicable federal laws, regulations, and business processes specific to U.S. federal agencies.

* Freedom of Information Act.

.

Part II

Corporation Comments and OIG Evaluation

CORPORATION COMMENTS AND OIG EVALUATION

The report contains six recommendations directed to the CPO. On January 4, 2007, the CPO provided a written response to a draft of this report, dated December 11, 2006. The CPO's response is presented, in its entirety, beginning on page II-4. The CPO concurred with all six of the report's recommendations. Based on the CPO's response, all six recommendations are considered resolved, but they will remain open until we have determined that agreed-to corrective actions have been completed and are effective. The CPO's response to each of the report's recommendations is summarized below, along with our evaluation of the response.

Recommendation 1: Enhance the FDIC's privacy program by integrating key ongoing and planned program control activities into a formally documented plan.

CPO Response: The CPO concurred with the recommendation. The CPO will enhance the existing program plan to formally document and describe the Corporation's privacy program goals and objectives, performance measures, organization and relationships of key initiatives, training and awareness strategy, and methods for reporting by December 15, 2007.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 2: Implement additional measures to ensure IIF is properly secured. Such measures could include performing periodic, unannounced walkthroughs of FDIC facilities and reporting the results to appropriate management officials.

CPO Response: The CPO concurred with the recommendation. The CPO will discuss appropriate, additional control measures for securing IIF with the CIO Council by April 15, 2007. A plan for implementing these measures will be completed by July 15, 2007. The plan will identify the date for final implementation of the measures.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 3: Place additional emphasis on employee and contractor awareness to physically safeguard IIF in their custody as previously discussed in this report.

CPO Response: The CPO concurred with the recommendation. The CPO recognizes the importance of employee and contractor privacy awareness and has taken actions to address this need at the FDIC. Such actions include privacy awareness training, Web site

materials, conference presentations among FDIC divisions and offices, and the promulgation of privacy policies and procedures. In addition, the CPO stated that Division of Resolutions and Receiverships (DRR) staff in Washington D.C., and DRR and Division of Supervision and Consumer Protection (DSC) staff in Dallas have received business-unit-specific privacy training. However, the CPO agreed to take several additional actions to further emphasize employee and contractor awareness regarding the physical safeguarding of IIF in their custody by November 30, 2007. Such actions include placing additional emphasis on physically safeguarding IIF during CIO Council meetings and Information Security Manager (ISM) meetings, including an item in the FDIC newsletter, and working with the FDIC's Office of Enterprise Risk Management (OERM) to develop a program for determining whether physical documents containing IIF are adequately secured.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 4: Review all PIAs posted on the FDIC's public Web site to determine whether they disclose all types of IIF used by the application and sufficiently describe the FDIC's use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

CPO Response: The CPO concurred with the recommendation. The CPO stated that the recommended actions are part of the FDIC's standard, ongoing processes. However, the CPO will perform a review of all currently posted PIAs to ensure that they adequately disclose all types of IIF used by the application and sufficiently describe the FDIC's use of IIF consistent with OMB policy and section 508 of the E-Government Act of 2002. The review will be completed, and any necessary corrections made, by March 15, 2007.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 5: Enhance current processes for preparing and publicly posting PIAs to ensure that new PIAs adequately describe the FDIC's collection and use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

CPO Response: The CPO concurred with the recommendation. The CPO stated that the recommended actions are part of the FDIC's standard, ongoing processes. However, the CPO will review current PIA posting processes to ensure that new PIAs adequately describe the FDIC's collection and use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002. The review will be completed, and any required adjustments made, by March 15, 2007.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

Recommendation 6: Enhance the FDIC's SDLC processes to fully address privacy considerations.

CPO Response: The CPO concurred with the recommendation. The CPO stated that the FDIC's RUP® SDLC addresses privacy considerations through the ASA, which determines whether IIF is in an application undergoing design. If IIF is present, a PIA is required. The CPO indicated that the PIA is used throughout the life cycle of a project, including during the development of requirements and performance of risk assessments and security testing and evaluation. However, the CPO recognizes that development teams may benefit from additional resources to ensure full attention to privacy issues. Accordingly, the CPO will add privacy roles and responsibilities to the intersecting organizations' portion of the FDIC's SDLC process by June 15, 2007.

OIG Evaluation of Response: The CPO's response satisfies the intent of the recommendation. The recommendation will remain open until we have determined that agreed-to corrective action has been completed and is effective.

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500
Division of Information Technology

December 11, 2006

MEMORANDUM TO: Russell A. Rau, Assistant Inspector General for Audits
Office of Inspector General

FROM: Michael E. Bartell
Chief Privacy Officer (CPO),
Chief Information Officer, and
Director, Division of Information Technology (DIT)

SUBJECT: Draft Audit Report Entitled, *The FDIC's Compliance with Section 522 of the Consolidated Appropriations Act, 2005* (Assignment 2006-027)

Thank you for the opportunity to respond to the draft report entitled, *The FDIC's Compliance with Section 522 of the Consolidated Appropriations Act, 2005.* The Chief Privacy Officer (CPO) appreciates the professional efforts of the FDIC Office of Inspector General (OIG) and their contractor KPMG LLP (KPMG) during this mandated independent third party review of the FDIC's privacy program and practices.

Consistent with the two prior privacy audits completed in September of this year, the draft report appropriately notes that the FDIC has implemented many actions to establish the agency's privacy program and to protect information in an identifiable form (IIF). Significant accomplishments in the draft report include the appointment of a Chief Privacy Officer (CPO), issuance of corporate policies and procedures for safeguarding IIF, the addition of a Privacy statement on the FDIC's Web site, completion of Privacy Impact Assessments (PIAs) on FDIC systems identified as containing IIF, completion of required Privacy Act-related reviews, and the implementation of mandatory Web-based privacy awareness training for FDIC employees and contractors. In addition, as noted by the OIG in the body of the draft report and in Appendix IV, the FDIC has 14 other key privacy initiatives already in process to further strengthen and improve the FDIC's policies, procedures, and practices and ensure compliance with federal privacy-related statutes, policies and guidelines.

The CPO further appreciates the OIG's recognition that the protection of IIF from unauthorized disclosure has been, and continues to be a Government-wide challenge and a significant concern to both the public and Congress. The CPO recognizes this challenge and is dedicated to ensuring continued confidence in the FDIC's privacy program and the agency's protection of IIF now and in the future. The OIG's observations warranting management's continued attention and the recommendations suggesting how the FDIC may further strengthen its privacy program will assist the agency in meeting those challenges.

Report recommendations: The CPO has carefully considered each of the six OIG recommendations which suggest how the FDIC may further protect IIF. The OIG Report on compliance with Section 522 recommends that the CPO should:

Recommendation #1:

- Enhance the FDIC's privacy program by integrating key ongoing and planned program control activities into a formally documented plan.

Response to Recommendation #1:

- **Concur.** The CPO will enhance the existing program plan to formally document and describe the Corporation's privacy program goals and objectives, performance measures, organization and relationships of key initiatives, training and awareness strategy, and methods for reporting by December 15, 2007.

Recommendation #2:

- Implement additional control measures to ensure IIF is properly secured. Such measures could include marking documents containing IIF and performing periodic, unannounced walkthroughs of FDIC facilities and reporting the results to appropriate management officials.

Response to Recommendation #2:

- **Concur.** The CPO will discuss with the CIO Council the appropriate additional control measures to ensure IIF is properly secured. These measures will be discussed with the Council by April 15, 2007 and will be documented in the minutes of the Council. A plan for implementing these measures will be completed by July 15, 2007. This plan will identify the date for final implementation of the measures.

Recommendation #3:

- Place additional emphasis on employee and contractor awareness to physically safeguard IIF in their custody as previously discussed in this report.

Response to Recommendation #3:

- **Concur:** The CPO recognizes the importance of employee and contractor privacy awareness and has taken action to address that need in the FDIC including privacy awareness training, website materials, conference presentations among the divisions and offices and the promulgation of privacy policies and procedures across the Corporation. Awareness is one part of a comprehensive privacy program and the CPO has addressed privacy awareness as aggressively as possible in the context of other privacy program requirements. For example, all staff in DRR and DSC in Dallas, as well as DRR in Washington, DC, received mandatory,

business unit-specific, privacy training. The most recent training was completed the week of November 20, 2006. These sessions stressed physical security to protect sensitive data both within the office and "on the road". Nevertheless, the CPO agrees to take the following actions by November 30, 2007, to further emphasize employee and contractor awareness regarding the physical safeguarding of IIF in their custody:

- Complete the series of planned privacy briefings to DSC and DRR;
- Include the physical safeguarding of IIF in periodic Information Security Manager meetings;
- Include the physical safeguarding of IIF in periodic CIO Council meetings;
- Include the physical safeguarding of IIF as an item in the FDIC Newsletter; and
- Work with the Office of Enterprise Risk Management to develop a program for determining whether physical documents containing IIF are adequately secured. At a minimum, the following will be performed:
    - By April 30, 2007 OERM will include special emphasis and reporting requirements for privacy in its guidance to management for preparing the 2007 Assurance Statements.
    - By November 30, 2007 "walk throughs" will be conducted to test whether physical documents containing IIF are adequately secured. This control measure also addresses recommendation two.

Recommendation #4:

- Review all PIAs posted on the FDIC's public Web site to determine whether they disclose all types of IIF used by the application and sufficiently describe the FDIC's use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

Response to Recommendation #4:

- **Concur.** The recommended actions are part of our standard, ongoing process that is already implemented. However, the CPO will complete a review of all the currently posted PIAs to ensure that they adequately disclose all types of IIF used by the application and sufficiently describe the FDIC's use of the IIF consistent with OMB policy and section 208 of the E-Government Act of 2002. This review will be completed and corrections made, if necessary, by March 15, 2007.

Recommendation #5:

- Enhance current processes for preparing and publicly posting PIAs to ensure that new PIAs adequately describe the FDIC's collection and use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002.

Response to Recommendation #5:

- **Concur.** The recommended actions are part of our standard, ongoing process that is already implemented. However, the CPO will review our current PIA posting process to ensure that new PIAs adequately describe the FDIC's collection and use of IIF consistent with OMB policy and section 208 of the E-Government Act of 2002. This review will be completed and any adjustments required to our current PIA posting process will be made by March 15, 2007.

Recommendation #6:

- Enhance the FDIC's SDLC processes to fully address privacy considerations.

Response to Recommendation #6:

- **Concur:** The FDIC's RUP SDLC currently addresses privacy considerations. As noted in the draft report, one of the earliest required artifacts and respective milestones within the RUP methodology is the Application Security Assessment (ASA). The ASA determines whether there will be personally identifiable information (PII) in the application undergoing design. If there is, a privacy impact assessment (PIA) is required. The PIA is used throughout the lifecycle of the project, including the development of requirements, the ongoing risk assessment, and the security test and evaluation. Nevertheless, the CPO understands the OIG's concern that development teams may benefit from additional resources to ensure full attention to privacy issues. As such, the CPO will add privacy roles and responsibilities to the intersecting organizations portion of the SDLC process to provide such information to development teams. The privacy intersecting organization material will be included by June 15, 2007.

As is customary, we will be happy to further discuss with the OIG any of these responses, and thank you for sharing your conclusions of the audit team in assessing the FDIC compliance with Section 522 of the Consolidated Appropriations Act. We believe this report affirms many of the considerable accomplishments of our program and look forward to continuing to build on aspects of our corporate privacy program in the coming year. Thank you.

cc: Ned Goldberg (DIT)
Steven Anderson (DIT)
Rack Campbell (DIT)
James Angel, Jr. (OERM)

MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents management's responses to the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The CPO will enhance the existing program plan to formally document and describe the Corporation's privacy program goals and objectives, performance measures, organization and relationships of key initiatives, training and awareness strategy, and methods for reporting.	December 15, 2007	N/A	Yes	Open
2	The CPO will develop a plan for implementing additional control measures for safeguarding IIF.	July 15, 2007	N/A	Yes	Open
3	The CPO will (a) complete planned privacy briefings to DSC and DRR, (b) place additional emphasis on physically safeguarding IIF during CIO Council and ISM meetings, (c) promote awareness through the FDIC newsletter, and (d) work with OERM to develop a program for determining whether physical documents containing IIF are adequately secured.	November 30, 2007	N/A	Yes	Open
4	The CPO will review all posted PIAs to ensure that they adequately disclose all types of IIF used by the application and sufficiently describe the FDIC's use of IIF.	March 15, 2007	N/A	Yes	Open
5	The CPO will review the FDIC's PIA posting process to ensure that new PIAs adequately describe the FDIC's collection and use of IIF.	March 15, 2007	N/A	Yes	Open

6	The CPO will add privacy roles and responsibilities to the intersecting organizations' portion of the SDLC process.	June 15, 2007	N/A	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(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] Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.