Office of Inspector General

Office of Audits
Report No. AUD-11-014

The FDIC's Privacy Program—2011

September 2011

Office of Inspector General

Executive Summary

The FDIC's Privacy Program—2011

Report No. AUD-11-014
September 2011

Why We Did The Audit

The FDIC Office of Inspector General (OIG) engaged the independent professional services firm of KPMG LLP (KPMG) to conduct an audit of the FDIC's privacy program. The objective of the audit was to assess the FDIC's privacy program and practices. The scope of the audit focused on the FDIC's processes for conducting and publicly posting Privacy Impact Assessments (PIA) and System of Records Notices (SORN) for information systems and collections of records that contain Personally Identifiable Information (PII). Specifically, KPMG's work focused on assessing the FDIC's compliance with the following:

- Section 208 of the E-Government Act of 2002 (Section 208) as it relates to performing PIAs;
- Provisions of the Privacy Act of 1974 (Privacy Act) related to SORNs and privacy policy disclosures;
- Requirements of Section 522 of Division H of the Consolidated Appropriations Act, 2005, as amended, for establishing a privacy program and supporting privacy policies; and
- Related privacy guidance established by the Office of Management and Budget (OMB) for SORNs and PIAs.

As part of the audit, KPMG selected a non-statistical sample of six collections of PII to assess whether the FDIC had conducted and publically posted the associated PIAs and SORNs consistent with relevant Federal privacy-related provisions in Section 208, the Privacy Act, and OMB guidance. In addition, KPMG selected two SORNs published by the FDIC in the *Federal Register* to determine whether the SORNs (a) had been approved by the FDIC's Board of Directors, (b) were published in the *Federal Register* at least 30 days prior to the collection and use of PII, and (c) satisfied the content requirements defined in the Privacy Act.

Background

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships, and in its role as a Federal employer and acquirer of services, the FDIC creates and acquires a significant amount of PII (e.g., names, Social Security numbers, or biometric records) related to depositors and borrowers at FDIC-insured financial institutions and FDIC employees and contractors. Implementing proper security controls over this PII is critical to mitigating the risk of an unauthorized disclosure that could lead to identity theft, consumer fraud, and potential legal liability or public embarrassment for the Corporation.

A number of Federal statutes establish requirements associated with analyzing how PII is handled, such as performing PIAs and making public notifications regarding completed PIAs and the categories of PII collected, maintained, retrieved, and used. A PIA is a process for (1) examining the risks and ramifications of using information technology to collect, maintain, and disseminate PII from or about members of the public and (2) identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. The public notification regarding completed PIAs and the categories of PII collected, maintained, retrieved, and used by the agency is referred to as a SORN.

Executive Summary

The FDIC's Privacy Program—2011

Report No. AUD-11-014
September 2011

Section 522 established the requirement that Federal agencies implement formal privacy programs. The statute requires agency Chief Privacy Officers (CPO) to have primary responsibility for the agency's privacy and data protection policy. As part of that responsibility, the CPO must assure the agency's use of technology sustains privacy protections. The CPO must also prepare an annual report to the Congress on the activities that affect privacy, including complaints of privacy violations, and implementation of related internal controls.

Audit Results

KPMG concluded that, except as noted below, the FDIC's privacy program and practices for processing PIAs and SORNs were compliant with selected provisions of Section 522, Section 208, the Privacy Act, and OMB guidance. Among other things, the FDIC had appointed a CPO with overall responsibility for the FDIC's privacy program and submitted annual privacy reports to OMB and the Congress as required by Section 522. Consistent with Section 208 and Privacy Act requirements, the FDIC had established processes for preparing PIAs and SORNs and making them publicly available and posted its privacy policies on the FDIC's public Web site. In addition, PIAs for five of the six PII collections sampled contained the required information regarding the FDIC's collection and use of PII. The one exception is described below. Moreover, the two SORNs that KPMG sampled had been properly approved by FDIC management, published in the *Federal Register*, and addressed the content requirements of the Privacy Act. Further, the FDIC included the required legal disclosures, referred to as a Privacy Act Statement, on all sampled forms that collect PII from the public in accordance with the Privacy Act.

While the above results are positive, KPMG also found that for three of the six PII collections sampled, the PIAs were not made available to the public until after the FDIC began collecting the PII. Additionally, the PIA covering one of the six sampled PII collections did not fully describe (a) what information was being collected, (b) the purpose of the collection, or (c) how the information was secured.

Recommendations and Management Comments

The report includes three recommendations intended to strengthen the Corporation's privacy program practices pertaining to PIAs and SORNs. Specifically, the report recommends that the CPO issue a corporate-wide policy requiring PIAs to be completed before collecting, maintaining, or disseminating PII. The report also recommends that the FDIC develop strategies for (1) elevating and reporting instances of non-compliance with privacy-related requirements to appropriate senior management officials who are in a position to ensure they are promptly and effectively resolved and (2) identifying and addressing instances of new PII collections that occur outside of the traditional systems development lifecycle that might require a PIA.

On September 12, 2011, the FDIC's Chief Information Officer (CIO), who also serves as the Director, Division of Information Technology, and CPO, provided a written response to a draft of this report. In the response, the CIO concurred with all three recommendations and described planned corrective actions that are responsive to the recommendations.

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

Office of Audits
Office of Inspector General

DATE: September 23, 2011

MEMORANDUM TO: Russell G. Pittman, Chief Information Officer,
Director, Division of Information Technology, and
Chief Privacy Officer

/Signed/
FROM: Mark F. Mulholland
Assistant Inspector General for Audits

SUBJECT: *The FDIC's Privacy Program—2011*
(Report No. AUD-11-014)

The subject final report is provided for your information and use. The FDIC Office of Inspector General (OIG) contracted with the independent professional services firm of KPMG LLP (KPMG) to perform the work. Please refer to the Executive Summary, included in the report, for the overall audit results. Our evaluation of your response is incorporated into the body of the report. Your comments on a draft of this report were sufficient to resolve the recommendations.

Consistent with the OIG's new approach to the Corrective Action Closure (CAC) process, the 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 the Office of Enterprise Risk Management (OERM) 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 OERM that corrective action is complete, but remain subject to follow-up at a later date.

If you have questions concerning the report, please contact me at (703) 562-6316 or Daniel Craven at (703) 562-6317. We appreciate the courtesies extended to the KPMG staff and OIG audit staff.

Attachment

cc: James H. Angel, Jr., Director, OERM
Bret D. Edwards, Director, DRR
Gary Jackson, Legal Division
Ned Goldberg, DIT
Rack Campbell, DIT
Steven B. Lott, DIT

Contents

Part I

Report by KPMG LLP

Audit of the FDIC's Privacy Program–2011

Prepared for the
Federal Deposit Insurance Corporation
Office of Inspector General

September 19, 2011

KPMG LLP
2001 M Street, NW
Washington, DC 2003

TABLE OF CONTENTS

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

EXECUTIVE SUMMARY

Honorable Jon T. Rymer
Inspector General
Federal Deposit Insurance Corporation
3501 N. Fairfax Drive
Arlington, VA 22226

Re: Transmittal of Results for the Audit of the FDIC's Privacy Program–2011

Dear Mr. Rymer:

This report presents the results of our independent audit of the Federal Deposit Insurance Corporation's (FDIC) privacy program and practices. This performance audit is intended, in part, to meet the requirements established by Section 522 of Division H of the Consolidated Appropriations Act, 2005, as amended and now re-codified to 42 United States Code (U.S.C.) § 2000ee-2 (Section 522). The audit objective was to assess the FDIC's privacy program and practices. The scope of the audit focused on the FDIC's processes for conducting and publicly posting Privacy Impact Assessments (PIA) and System of Records Notices (SORN) for information systems and collections of records that contain Personally Identifiable Information (PII).[1] Specifically, the audit included an assessment of the FDIC's compliance with the following:

(a) Section 208 of the E-Government Act of 2002 (Section 208)[2] as it relates to performing PIAs,
(b) Provisions of the Privacy Act of 1974 (Privacy Act) related to SORNs and privacy policy disclosures,
(c) Section 522 requirements for establishing a privacy program and supporting privacy policies, and
(d) Relevant privacy guidance established by OMB for SORNs and PIAs.

Our audit included a non-statistical[3] selection of six collections of PII pertaining to business processes within the Division of Resolutions and Receiverships (DRR). Within the FDIC, DRR has primary responsibility for planning and efficiently handling the resolution of failing financial institutions, including coordinating all efforts related to the analysis, valuation, marketing, and sale of failing or

[1] 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 information in an identifiable form (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, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements. OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* introduces the term PII as a replacement for IIF. Our report uses the term PII to be consistent with more recent OMB memoranda, such as OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* and National Institute of Standards and Technology (NIST) guidance.

[2] The E-Government Act requires an agency to take certain actions before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or initiating a new collection of information that will be collected, maintained, or disseminated using information technology; and includes any information in an identifiable form permitting the physical or online contacting of a specific individual. These actions include conducting, preparing, and generally making a PIA publicly available.

[3] A non-statistical sample is judgmental and, therefore, cannot be projected to the population.

failed institutions and associated assets such as residential mortgages, commercial loans, and other consumer loans. For each collection selected, we assessed whether the FDIC conducted and publicly posted the associated PIAs and SORNs consistent with relevant Federal privacy-related provisions in Section 208, the Privacy Act, and OMB guidance. We also reviewed the 2 most recent SORNs created within the last 3 years from a population of 32 SORNs.[4] The scope of the audit did not include an evaluation of access controls over PII collected and maintained by the FDIC as the Office of Inspector General (OIG) planned to evaluate these controls as part of its annual independent security evaluation required by the Federal Information Security Management Act (FISMA) of 2002.

On June 30, 2011, we shared our preliminary results with representatives of the Division of Information Technology (DIT), DRR, and Legal Division. In preparing our report, we considered feedback received from these officials.

We concluded that, except as noted below, the FDIC's privacy program and practices for processing PIAs and SORNs were compliant with selected provisions of Section 522, Section 208, the Privacy Act, and OMB guidance. Among other things, the FDIC had appointed a Chief Privacy Officer (CPO) with overall responsibility for the FDIC's privacy program and submitted annual privacy reports to OMB and the Congress as required by Section 522. Consistent with Section 208 and Privacy Act requirements, the FDIC established processes for preparing PIAs and SORNs and making them publicly available and posted its privacy policies on the FDIC's public Web site. In addition, PIAs for five of six PII collections sampled contained the required information regarding the FDIC's collection and use of PII. The one exception is described below. In addition, the two SORNs we sampled had been properly approved by FDIC management, published in the *Federal Register*, and addressed the content requirements of the Privacy Act. Further, the FDIC included the required legal disclosures, referred to as a Privacy Act Statement, on all sampled DRR forms that collect PII from the public in accordance with the Privacy Act.

While the above results are positive, we also found that for three of the six PII collections sampled, the PIAs were not made available to the public until after the FDIC began collecting the PII. Additionally, the PIA covering one of six sampled PII collections did not fully describe (a) what information was being collected, (b) the purpose of the collection, or (c) how the information was secured.

Our report includes recommendations intended to strengthen the Corporation's privacy program practices pertaining to PIAs and SORNs. Specifically, we are recommending that the CPO issue a corporate-wide policy requiring PIAs to be completed before collecting, maintaining, or disseminating PII. We are also recommending that the FDIC develop strategies for (1) elevating, reporting, and resolving instances of non-compliance with privacy-related requirements and (2) identifying instances of new PII collections that occur outside of the traditional systems development lifecycle that might require a PIA.

The American Institute of Certified Public Accountants (AICPA) developed the *Generally Accepted Privacy Principles (GAPP)* as a framework to help organizations proactively manage privacy risks. GAPP provides a set of recommended privacy practices to help organizations build effective privacy programs. FDIC management has voluntarily adopted aspects from the 10 principles of GAPP and incorporated those principles and associated practices into the FDIC's *Privacy Program Strategic Framework*, dated August 11, 2008. We compared the FDIC's privacy monitoring activities to one

[4] The prior 30 SORNs were created from 1975 to 2007. As these SORNs existed for a substantial amount of time prior to our audit, we did not select them for testing. We analyzed the more recent SORNS to obtain a more representative sample of the FDIC's current Privacy Act compliance practices. These two SORNs were FDIC-30-64-0032, *Nationwide Mortgage Licensing System and Registry,* and FDIC-30-64-0031, *Online Ordering Request Records.* They are publicly available at http://www.fdic.gov/regulations/laws/rules/2000-4050.html#fdictail.

GAPP principle, *Monitoring and Enforcement,* and the related criteria, controls, and procedures that can be used by an organization to monitor compliance with its privacy policies and procedures. As the FDIC is not required by policy or statute to implement GAPP, we have separately communicated the results of this comparison to the FDIC.

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 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 tested the FDIC's privacy processes that were implemented as of May 10, 2011. We caution that projecting the results of our audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Appendix I provides the objective, scope, and methodology of this performance audit; *Appendix II* lists significant criteria; *Appendix III* provides a list of acronyms; and *Appendix IV* provides a glossary of terms.

Sincerely,

KPMG LLP

September 19, 2011

BACKGROUND

What is Privacy?

The concept of "privacy" is one whose meaning differs depending on the individual, the culture, or the context of its use. From a legal perspective, "privacy" means "the right to be free of unnecessary public scrutiny or to be left alone."[5] Within the Federal Government, privacy refers to information about U.S. citizens and their right to privacy. Within that context, privacy is defined as the ability of a person to control the availability of information about them, especially information that may be used to uniquely identify that individual. Protecting this information and ensuring each individual's right to privacy is fundamental to promoting trust in Government and ensuring the rights of the people.

Balancing the need for protecting the privacy of U.S. citizens is the need for the U.S. Government to deliver services to beneficiaries of Government programs efficiently. Information systems provide the U.S. Government significant capabilities to deliver these services and benefit programs efficiently. Without the trust and confidence of the public to voluntarily share PII, most Government agencies could not efficiently and effectively carry out their program's mission. The growth in the collection of PII reflects the essential need for Government agencies to use PII. In the 2009 FISMA report to the Congress,[6] OMB reported that the number of Federal information systems collecting and processing PII increased 31 percent from 2007 to 2009. Parallel with the increase in the collection of PII are media reports of identity theft and massive losses of PII records, such as an incident that occurred at a Federal agency where a lost laptop contained PII on 26 million veterans.

Privacy Information at the FDIC

In its capacity as the Receiver of failing or failed financial institutions, the FDIC collects significant quantities of PII from failing or failed financial institutions. Such information includes, for example, sensitive PII, such as names, addresses, SSNs, phone numbers, dates of birth, and account and loan data for institution depositors, borrowers, and employees. The FDIC utilizes this sensitive PII in many resolution activities, such as paying depositor claims, valuing assets (e.g., loans) from failed institutions, and pursuing claims against individuals that contributed to the financial institution's failure.

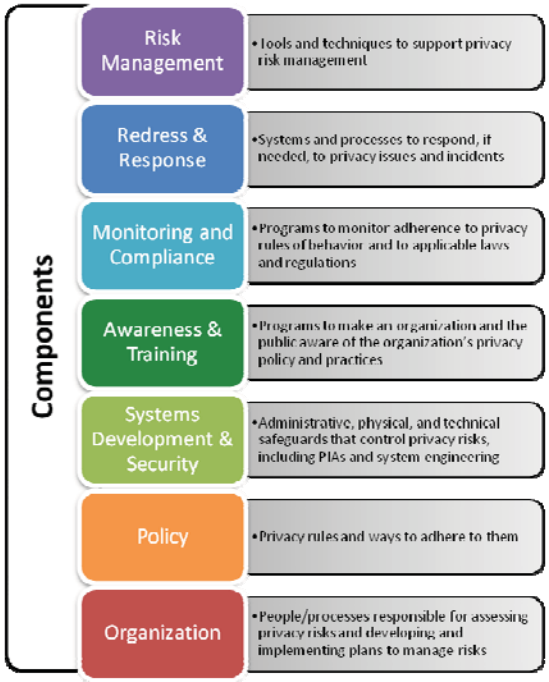
With the significant increase in resolution and receivership activity in 2009 and 2010, the FDIC contracted with third parties to perform many duties associated with closing financial institutions and selling acquired assets. To address the risks associated with vendors processing sensitive PII on the FDIC's behalf, the FDIC's Information Security and Privacy Staff (ISPS) began performing security and privacy risk assessments for vendors that process significant amounts of sensitive bank customer data. As part of each vendor privacy risk assessment, ISPS completed a 51-question privacy assessment, conducted an interview with the vendors, and prepared a vendor assessment report. ISPS also reported that it continued its practice of performing physical security walkthroughs in 2009 to identify unsecured PII.

[5] Nolo's Plain-English Law Dictionary.

[6] OMB's *Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* found at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf.

Characteristics of a Privacy Program

Government organizations must balance the implementation of mission objectives and business functions with risk. Maintaining this balance requires organizations to establish a privacy program encompassing multiple facets, such as an organization's people, processes, and technology. The exhibit *Privacy Program* depicts seven components of a privacy program found in leading organizations. An effective privacy program provides protection to information and information systems from unauthorized access, use, or disclosure in order to maintain the confidentiality of information. The confidentiality of information has a major impact on the operations and assets of an organization as well as the welfare of individuals.



Source: KPMG analysis of Federal privacy legislation and OMB requirements.

Federal Requirements for Privacy Programs

The passage of Section 522 in the Consolidated Appropriations Act of 2005 established the requirement that federal agencies implement formal Privacy Programs.[7] Prior to the passage of Section 522, many federal agencies divided implementation responsibilities for the Privacy Act and the E-Government Act with varying degrees of success. Congress recognized the need for agencies to unify disparate activities under a single program to improve efficiency and effectiveness; and thus it established the Privacy Program requirements in Section 522.

Section 522 requires the agency's CPO to have primary responsibility for agency privacy and data protection policies. As part of that responsibility, the CPO must assure that the agency's use of technology sustains privacy protections. The CPO must also prepare an annual report to the Congress on the activities that affect privacy, including complaints of privacy violations, and implementation of related internal controls.[8]

FDIC's Privacy Program and Chief Privacy Officer Roles and Responsibilities

The FDIC Chief Information Officer (CIO) serves as the CPO and reports directly to the FDIC Chairman. The CPO is a statutorily-mandated position and serves as the Senior Agency Official for Privacy responsible for establishing and implementing a wide range of privacy and data protection policies and procedures pursuant to various legislative and regulatory requirements. In executing these responsibilities, the CPO collaborates and consults with the FDIC's Legal Division; the divisional Information Security Managers; the Privacy Counterparts Committee; and individuals within the Division of Risk Management Supervision.[9]

[7] While Section 522 does not define "agency," the FDIC determined that the better course would be to comply with this Section.
[8] Annually, the FDIC CPO prepares and submits responses to OMB's privacy questions as part of the Corporation's FISMA report to OMB and the Congress. This annual submission satisfies Section 522 reporting requirements.
[9] During the audit period, the Division of Supervision and Consumer Protection changed their name to the Division of Risk Management Supervision effective February 13, 2011 to recognize its new and enhanced responsibilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act.

RESULTS OF AUDIT

We concluded that, excepted as noted later in the report, the FDIC's privacy program and practices for processing PIAs and SORNs were compliant with selected provisions of Section 522, Section 208, the Privacy Act, and OMB guidance. Among other things, the FDIC had appointed a CPO with overall responsibility for the FDIC's privacy program and submitted annual privacy reports to OMB and the Congress as required by Section 522. Consistent with Section 208 and Privacy Act requirements, the FDIC established processes for preparing PIAs and SORNs and making them publicly available and posted its privacy policies on the FDIC's public Web site. In addition, PIAs for five of six PII collections sampled contained the required information regarding the FDIC's collection and use of PII. The one exception is discussed later in the report. In addition, the two SORNs we sampled had been properly approved by FDIC management, published in the *Federal Register*, and addressed the content requirements of the Privacy Act. Further, the FDIC included the required legal disclosures, referred to as a Privacy Act Statement, on all sampled DRR forms that collect PII from the public in accordance with the Privacy Act.

While the above results are positive, we also found that for three of the six PII collections sampled, the PIAs were not made available to the public until after the FDIC began collecting the PII. Additionally, the PIA covering one of six sampled collections of PII did not fully describe (a) what information was being collected, (b) the purpose of the collection, or (c) how the information was secured.

Section 522 – Chief Privacy Officer, Policies, and Procedures

Section 522 of the Consolidated Appropriations Act of 2005, re-codified to 42 U.S.C. § 2000ee-2, is the most recent addition to the privacy statutory landscape that governs the privacy practices of Federal agencies. This legislation expands on the foundation and framework laid by the Privacy Act and the E-Government Act by instituting programmatic level requirements and re-enforcing the provisions of prior legislation.

Section 522 establishes two ongoing requirements for those Federal agencies that are bound by that Section. First, the agencies must appoint a CPO and delegate to that individual specific responsibilities related to privacy operations. Second, the agencies must establish comprehensive privacy and data protection policies and procedures that are consistent with regulatory guidance, including the Privacy Act, E-Government Act, and OMB guidance.

KPMG evaluated the FDIC's Privacy Program for compliance with selected Section 522 requirements. Specifically, KPMG determined whether the FDIC appointed a CPO, assigned responsibilities to the CPO consistent with the legislation, and developed policies and procedures to implement the Privacy Act and Section 208. For both the Privacy Act and E-Government Act, KPMG determined whether the FDIC's written policies and procedures addressed the legislative requirements of the Privacy Act, Section 208, and Section 522.

In March 2005, the FDIC appointed a senior official, the 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. Through the Privacy Program Office, the FDIC has instituted a mandatory, online annual privacy-training program for all employees and all contractors who have access to the FDIC's internal network. Supplementing the annual privacy training are periodic email reminders from the FDIC CIO to safeguard sensitive information, including PII, and privacy awareness posters posted adjacent to shared printers and copiers. Further, to promote the secure destruction of sensitive information, the FDIC has placed shred bins in hallways throughout the FDIC's Washington, D.C., and Virginia Square offices.

Section 208 – Privacy Impact Assessments

Section 208 includes requirements for Federal agencies to conduct PIAs prior to initiating a new collection of PII or developing or procuring information technology (IT) systems or projects that collect, maintain, or disseminate information in an identifiable form from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in an identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the Federal Government). PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. Additionally, if practical, completed PIAs should be made publicly available through the Web site of the agency, publication in the *Federal Register*, or other means. Section 208 also 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. The FDIC has determined that the Corporation is subject to the above provisions of Section 208.

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act*, dated September 26, 2003, provides guidance for implementing provisions of Section 208. Among other things, the OMB memorandum provides details on the required content of PIAs.[10] Specifically, the memorandum states that agencies must conduct reviews of how information about individuals is handled within their agency and that agencies must prepare PIAs, which 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). OMB states that Memorandum M-03-22 applies to agencies and their contractors that use IT or that operate Web sites for purposes of interacting with the public.

The FDIC has established policies and procedures that require divisions and offices to complete a privacy questionnaire, referred to as a Privacy Threshold Analysis (PTA), whenever new information systems[11] are developed or acquired. Specifically, the FDIC's procurement policy requires FDIC divisions and offices to complete PTAs when contracting for IT. The purpose of the PTA is to help the Privacy Program Office determine whether the information system contains (a) public sensitive PII and is subject to Section 208's PIA requirement (external PIA) or (b) employee/contractor sensitive PII and is subject to internal FDIC procedures for preparing PIAs (internal PIA). PTAs are submitted to, and analyzed by, the Privacy Program Office.

For systems that are subject to Section 208 and/or FDIC internal procedures, the division or office sponsoring the IT project or acquisition must prepare a PIA. A single PIA may cover one or more PII collections (see the following table for examples). The division or office is responsible for providing completed PIAs to the Privacy Program Office for review and approval. When a PIA for a system containing public sensitive PII is approved by the Privacy Program Office and CPO, the PIA is made available to the public through a notice posted on the FDIC's public Web site.[12] Additionally, PIAs for systems containing employee/contractor sensitive PII are posted on FDIC's internal Privacy Program Web site as a best practice. Both external and internal PIAs are approved by the CPO or designee.

We selected six collections of PII and assessed whether the associated PIAs (a) contained required information describing the FDIC's collection and use of the PII and (b) were completed and made publicly available before the FDIC began collecting the PII. We found that for five of the six collections, the associated PIAs contained sufficient information regarding the collection or use of the PII. However,

[10] Section 208 delegates to the OMB Director the responsibility to develop specific implementation requirements for the provisions of the legislation.

[11] The E-Government Act of 2002 defines an "information system" as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See 44 U.S.C. § 3502(8). According to the FDIC's PTA form, all technologies/systems should be initially reviewed for potential privacy impact.

[12] The availability of the FDIC's PIAs are posted at http://www.fdic.gov/about/privacy/assessments.html. Interested citizens may request a specific PIA for review by email to privacy@fdic.gov.

information regarding the collection and use of PII for the remaining collection was not sufficiently described in the associated PIA. We also noted that the PIAs had not been completed and made publicly available before the FDIC began collecting PII for three of the six collections. Notably, as described below, one of these three exceptions involved an information system established in 1997, which pre-dated the requirement for conducting PIAs. As of May 10, 2011, the FDIC had taken action to make PIAs covering all six PII collections publicly available. The table summarizes the PII collections that we selected and the results of our analysis. A more detailed discussion of the exceptions we found follows the table.

Summary Analysis of Section 208 Compliance for Selected Collections of PII

	PII Collection	Associated PIA That Addresses the PII Collection	Did the PIA Contain Information Regarding the Collection and Use of PII?	Was the Information Regarding the PII Collection and Use Available to the Public Prior to its Collection?
1	Depositor claims for a closed financial institution.	Claims Administration System (CAS) PIA	Yes	Yes
2	Depositor liabilities information obtained from failed institution information system during Pre-close phase.	CAS PIA	Yes	Yes
3	Professional liability claims against directors and officers of failed financial institutions.	DRR Locations and Reporting System (DOLLARS) PIA	Yes	Not Applicable – Pre-2002*
4	Digital images of loan files for cash asset sales.	PIA for a confidential financial advisory firm's ShareVault system	Yes	No
5	Loan file images maintained by DRR's Asset Marketing for the valuation of assets by third-party asset valuation contractors.	PIA for a confidential IT provider's Virtual Data Room system	Yes	No
6	Persons of Interest (POI) collection maintained by DRR's Investigations Unit.	DOLLARS PIA	In Part	In Part

Source: KPMG analysis of the FDIC's procedures pertaining to the six selected PII collections as of May 10, 2011. The Privacy Program Office identified the four PIAs referenced above as covering the six selected collections.
* DOLLARS began processing PII in 1997, approximately 6 years before Section 208 required Federal agencies to complete PIAs and make them publicly available.

Timeliness of PIAs

We identified the following three exceptions regarding the timeliness of PIAs.

Digital Images of Loan Files for Cash Asset Sales (ShareVault)
The FDIC, as Receiver for failed financial institutions, assumes the task of collecting and selling assets from failed financial institutions. The FDIC contracted with a financial advisory firm that specializes in conducting online auctions of loans from failed institutions to qualified bidders. On behalf of the FDIC, the financial advisory firm utilized a proprietary system, called ShareVault, to process and maintain digital images of loan files for cash sales to qualified bidders. These loan files contained PII, such as SSNs, dates of birth, drivers' licenses, bank account numbers, tax returns, credit reports, and employment information. DRR began collecting PII and using the ShareVault system in October 2009 to market the assets from a failed financial institution. The PIA was made publicly available on May 3, 2011, approximately 19 months after the FDIC began collecting and storing PII in the ShareVault system.

Loan File Images Maintained by DRR's Asset Marketing for the Valuation of Assets by Third-Party Asset Valuation Contractors (Virtual Data Rooms)
In its capacity as Receiver for failed financial institutions, the FDIC contracted with an IT provider to provide a private data-sharing environment, called Virtual Data Rooms, to facilitate the exchange of data between the FDIC and third parties. The FDIC utilized these Virtual Data Rooms to market billions of dollars in assets. The Virtual Data Rooms contained significant quantities of PII, such as borrower names, SSNs, dates of birth, and home addresses, in digital loan files. Valuation contractors used the Virtual Data Rooms and accompanying digital loan files to support Structured Asset Sales transactions by the FDIC.

The FDIC did not store PII in Virtual Data Rooms when it began using them in September 2000. DRR officials had begun using Virtual Data Rooms to maintain PII in the fall of 2008. The PIA associated with the Virtual Data Rooms was finalized and made publicly available on May 10, 2011, approximately 30 months after the FDIC began collecting and storing PII in Virtual Data Rooms.

Persons of Interest (POI) Collection Maintained by DRR's Investigations Unit
DRR maintains this PII collection in a password-protected Excel spreadsheet and uses it to track directors, officers, mortgage brokers, real estate agents, appraisers, and others who are suspected of contributing to the failure of financial institutions. Investigators access the spreadsheet when screening potential FDIC employees and contractors. As of January 27, 2011, the spreadsheet contained the names, SSNs, and dates of birth for approximately 4,600 individuals. According to DRR officials, many of the individuals contained in the POI collection were not stored in DOLLARS[13] or any other FDIC information system as of January 2011. The investigators indicated that they developed the spreadsheet because DOLLARS did not have the capability to efficiently compare groups of potential FDIC employees and contractors against the names stored in DOLLARS. This POI collection was initiated after the completion of the DOLLARS PIA. In addition, the PIA had not been updated to include the new intended use, the new PII data type collected (i.e., date of birth), or associated protections taken to secure the POI collection.

Section 208 requires Federal agencies, including the FDIC, to conduct PIAs of information systems and collections and, in general, make PIAs publicly available before—

[13] The FDIC identified the DOLLARS PIA as covering the POI Collection Maintained by the DRR Investigations Unit.

1. Developing or procuring IT that collects, maintains, or disseminates PII; or
2. Initiating a new collection of information that—
   a. will be collected, maintained, or disseminated using IT; and
   b. includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements were imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

Additionally, OMB Memorandum M-03-22 supplements Section 208 requirements for preparing and making a PIA publicly available and indicates that PIA requirements apply to "agencies and their contractors that use information technology or that operate Web sites for purposes of interacting with the public." The FDIC formally assessed the PII collections in the financial advisor's ShareVault system and the IT provider's Virtual Data Rooms using a PTA and determined that both systems were subject to Section 208 requirements and required a PIA. However, Privacy Program staff advised us that the PIA requirements of Section 208 are not legally binding with respect to the ShareVault system and Virtual Data Rooms because the systems provide an "information service" that does not meet the intent of "developing or procuring information technology that collects, maintains, or disseminates PII" as referenced in Section 208. Nevertheless, the officials did recognize privacy risks associated with these systems and indicated that, as a best practice, the FDIC requires that PIAs be performed for all vendors maintaining sensitive PII data on behalf of the Corporation.

Several factors contributed to the conditions described above. Some of the factors were specific to the PII collections and systems that we reviewed, while others were broader in nature.

Virtual Data Rooms

DRR officials began using Virtual Data Rooms to maintain PII in the fall of 2008, but did not notify the Privacy Program Office of this change in business practice. The Privacy Program Office identified the need for a PIA in February 2009 while conducting an internal assessment, and subsequently communicated this need in a report to DRR management.[14] DIT did not identify the need for a PIA before 2009 because the storage of PII in Virtual Data Rooms did not require a software modification and, therefore, was not subject to the FDIC's software development process, called Rational Unified Process (RUP®). RUP® includes procedures for ensuring that a PIA is developed whenever an application processes sensitive PII. DRR provided the Privacy Program Office with a draft PIA on May 27, 2009. The PIA was approved and made publicly available in May 2011.

The Office of the Inspector General (OIG) previously identified the need to complete a PIA for Virtual Data Rooms and make it publicly available in its report on the *Independent Evaluation of the FDIC's Information Security Program—2009* (AUD-10-001), dated November 2009. The report noted that DIT could help mitigate the risk of a similar situation recurring by emphasizing in awareness and training materials the importance of consulting with the Privacy Program Office before using PII in information systems. In response, DIT took actions in June 2010 by developing additional privacy training.

[14] *Privacy/Security Assessment of the Division of Resolutions and Receiverships' (DRR) Bank Resolution Pre-Closing Process*, dated April 23, 2009.

ShareVault System

DRR informally determined that a PIA was needed for the financial advisor's ShareVault system in July 2009, which was 3 months before ShareVault began processing PII. According to a DRR information security professional, due to higher-priority concerns with the ongoing crisis in the banking sector, DRR did not prepare a PIA for the ShareVault system when it began processing PII in October 2009. DRR provided a draft PIA to the Privacy Program Office in February 2010. The PIA was approved and made publicly available in May 2011.

General Factors

With respect to contractor-operated information systems and/or services (such as the Virtual Data Rooms and the ShareVault system), a Privacy Program staff member advised us that project teams generally submit draft PIAs to the Privacy Program after (rather than before) the contract is awarded and the vendor begins processing data on behalf of the FDIC. The FDIC does not have a corporate-wide policy requiring FDIC divisions and offices to publish PIAs prior to the implementation of a vendor-operated system or service. As previously stated, RUP® includes procedures for ensuring that a PIA is developed for applications that process PII. However, contractor-operated information systems and/or services are typically not subject to RUP®.

Privacy Program staff advised us that they were working to develop a corporate-wide policy[15] that would describe the roles, responsibilities, and circumstances surrounding when PIAs are required. This policy could include a requirement for divisions and offices to finalize PIAs before FDIC or contractor-operated systems and/or services collect, maintain, or disseminate PII. Such a requirement would be consistent with Section 208 requirements.

As of April 2011, the Privacy Program Office was tracking and working to address eight additional information systems that were processing PII without a completed and publicly available PIA.[16] Although not required by statute or policy, the FDIC may find it beneficial to develop a strategy for elevating, reporting, and resolving instances of non-compliance with privacy-related requirements, including PIA requirements. Such a strategy, which could be referenced in the corporate-wide policy discussed above, would help focus management attention on the need for prompt action in resolving instances of non-compliance with privacy requirements when competing priorities exist. It may also help mitigate delays in completing PIAs, such as those experienced with the financial advisor's ShareVault system and the IT provider's Virtual Data Rooms.

PIAs are intended to promote the public trust through increased transparency and assurances that personal information maintained by or for a Federal agency is protected. When PIAs are not completed and made available to the public in a timely manner, it reduces the FDIC's assurance that it had performed the necessary risk assessment and informed the public, in a timely manner, of the FDIC's collection and use of the information.

[15] Draft FDIC Circular, entitled *Privacy Impact Assessment Requirements*.

[16] These systems were not part of our sample. Six of the eight systems involved applications dealing with secure email, email archival solutions, voicemail, and other communication technologies with the public. The Privacy Program staff are evaluating alternatives for presenting the information for these six systems to either the public or employees. For the remaining two systems involving public PII, the PIAs are expected to be completed by year-end according to Privacy Program staff.

Recommendations

We recommend that the CPO:

1. Finalize and issue the draft corporate policy on PIA requirements and include clarifying language in the policy that requires PIAs to be completed and publicly available before collecting, maintaining, or disseminating PII.

2. Enhance Privacy Program controls by defining a strategy for elevating and reporting instances of non-compliance with relevant Federal privacy requirements to appropriate senior management officials who are in a position to ensure they are promptly and effectively resolved.

Content of PIAs

PIAs for five of the six PII collections that we reviewed described the FDIC's collection and use of PII and identified the associated SORN. However, the PIA for the remaining collection—POI Collection maintained by the DRR Investigations Unit—did not fully describe (a) what information was being collected, (b) the purpose of the collection, or (c) how the information was secured. The FDIC identified the DOLLARS PIA as covering the POI Collection maintained by the DRR Investigations Unit. The POI Collection maintained by the DRR Investigations Unit resides in a password-protected Excel spreadsheet that was developed by DRR investigators to track directors, officers, mortgage brokers, real estate agents, appraisers, and others suspected of contributing to the failure of financial institutions. Investigators access the spreadsheet when screening potential FDIC employees and contractors. The investigators advised us that, as of January 2011, the POI collection contained specific PII information that was not in DOLLARS or any other FDIC information system. As of January 2011, the spreadsheet contained the names, SSNs, and dates of birth for approximately 4,600 individuals.

Section 208 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 detailed information regarding the required content of PIAs. 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).

The Privacy Program Office did not identify the need to update the DOLLARS PIA for the POI Collection because DRR officials did not identify the POI spreadsheet as a new collection of PII. Additionally, the spreadsheet was not subject to the RUP® software development process and the associated analysis for potential privacy requirements.

FDIC officials advised us that employees and contractors often create spreadsheets and databases using data from FDIC information systems for the purpose of facilitating analysis. Such spreadsheets are generally covered by existing PIAs. However, in the case of the spreadsheet described above, the data was not derived from another FDIC information system. Rather, it was derived from failed financial institution files, and the PII collection was not covered by an existing PIA.

We recognize that it is not cost-beneficial to conduct a review of every spreadsheet or database that an FDIC employee or contractor creates to determine whether a PIA is required. However, the FDIC could benefit from developing a strategy to help identify and address instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA. Such a strategy could

consist of increased emphasis in the FDIC's annual privacy awareness materials regarding the importance of contacting the Privacy Program Office when creating new PII collections, conducting periodic reviews to identify such collections, and/or enhancing the Privacy Program Office's ongoing monitoring activities to help identify data collections outside of the systems development life cycle.

Absent an update to the DOLLARS PIA that addresses information related to the POI Collection by the DRR Investigations Unit, the FDIC has reduced assurance that it has adequately assessed the risk of collecting, monitoring, and using the information and informed the public, in a timely manner, of the FDIC's collection and use of the information.

Subsequent to sharing our preliminary audit results with the FDIC on June 30, 2011, the Privacy Program Office revised the DOLLARS PIA to incorporate the POI Collection maintained by the DRR Investigations Unit and made it publicly available on July 25, 2011. We are, therefore, making no recommendation regarding the need for a PIA for this PII collection.

Recommendation

We recommend that the CPO:

3. Develop a strategy to help identify and address instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA.

Privacy Act - System of Records Notices

The Privacy Act includes requirements for Federal agencies, including the FDIC, to inform the public of the existence of systems of records that contain PII and to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records."[17] For the purposes of the Privacy Act, a system of records is "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[18]

The Privacy Act also requires that agencies publish a notice "upon the establishment or revision" of a system of records. OMB has determined that the notice must be published before the system or records becomes "operational." OMB's original interpretation of "operational" meant, "Before any information about individuals is collected." In 1996, OMB clarified that interpretation so that it applies to the collection and use of the information. Additionally, if the agency is publishing a new "routine use" of the information in the system or records, the notice must be published at least 30 days before the release of the information."[19] At the FDIC, SORNs are published after authorization by the Board of Directors.

We selected two SORNs published by the FDIC in the *Federal Register* to determine whether the SORNs (a) had been approved by the FDIC's Board of Directors, (b) were published in the *Federal Register* at least 30 days prior to the collection and use of PII, and (c) satisfied the content requirements defined in the Privacy Act.[20] These two SORNs were FDIC-30-64-0032, *Nationwide Mortgage Licensing System and Registry,* published on March 21, 2011; and FDIC-30-64-0031, *Online Ordering Request Records*, published on October 26, 2009.

We determined that the Board had approved the SORNs for both systems prior to being published in the *Federal Register* and that the SORNS were published with appropriate notice and addressed the content requirements of the Privacy Act.

[17] The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10).
[18] The Privacy Act of 1974, 5 U.S.C. § 552a(a)(5).
[19] See id., § 552a(e)(4) and (e)(11), and OMB's Privacy Act Guidelines (published July 9, 1975) as well as Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals* to OMB Circular No. A-130 (published February 20, 1996).
[20] KPMG assessed the nine required elements of a SORN: 1) system location and name; 2) categories of individuals covered by the system; 3) categories of records in the system; 4) purpose and routine uses of records maintained; 5) policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system; 6) system manager and address; 7) notification and records access procedure; 8) contesting record procedure; and 9) record source categories. *Federal Register, Vol. 74,* (October 26, 2009).

APPENDIX I – OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to assess the FDIC's privacy program and practices. Specifically, the audit included an assessment of the FDIC's compliance with the following:

(a) Section 208 of the E-Government Act of 2002 (Section 208) as it relates to performing PIAs,
(b) Provisions of the Privacy Act of 1974 (Privacy Act) related to SORNs and privacy policy disclosures,
(c) Section 522 requirements for establishing a privacy program and supporting privacy policies, and
(d) Related privacy guidance established by OMB for SORNs and PIAs.

Scope

As required by our task assignment with the FDIC OIG, KPMG evaluated the FDIC's compliance with Federal privacy-related statutes and other criteria agreed upon with the OIG. KPMG completed a formal analysis of Federal privacy-related statutes and relevant FDIC policy to identify areas that KPMG would use to assess the FDIC's compliance with Section 522, the Privacy Act of 1974, Section 208 of the E-Government Act, and OMB Memorandum M-03-22 *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (OMB M-03-22).

Based on the analysis of privacy criteria, the scope of the audit focused exclusively on the following areas listed below:

1. Establishment of a Privacy Program
2. Policies and Procedures for Privacy
3. System of Record Notices (SORNs)
4. Privacy Impact Assessments (PIAs)
5. Privacy Policy Disclosure
6. Privacy Act Statements

KPMG selected the above areas for testing as Section 522 makes multiple references to the Privacy Act of 1974, Section 208, and OMB M-03-22. KPMG prioritized its testing to determine compliance with key provisions of Section 522, Privacy Act, E-Government Act and/or OMB regulations. The audit did not include an evaluation of access controls over PII collected and maintained by the FDIC as the OIG planned to evaluate these controls as part of its annual FISMA audit.

Our audit included a non-statistical[21] selection of six collections of PII pertaining to business processes within DRR. For each collection, we assessed whether the FDIC conducted and publicly posted the associated PIAs and SORNs consistent with relevant Federal privacy-related requirements in Section 208, the Privacy Act, and OMB guidance. We also analyzed the two most recent SORNs created within the last 3 years from a population of 32 SORNs.

The AICPA developed the GAPP as a framework to help organizations proactively manage privacy risks. GAPP provides a set of recommended privacy practices to help organizations build effective privacy programs. The FDIC's Privacy Program has voluntarily adopted aspects from the 10 principles of GAPP and incorporated those principles and associated practices into the FDIC's *Privacy Program Strategic Framework*, dated August 11, 2008. We compared the FDIC's monitoring activities to one GAPP principle, *Monitoring and Enforcement,* and the related criteria, controls, and procedures that can be used

[21] A non-statistical sample is judgmental and, therefore, cannot be projected to the population.

by an organization to monitor compliance with its privacy policies and procedures. As the FDIC is not required by policy or statute to implement GAPP, we have separately communicated the results of this analysis to the FDIC.

KPMG did not perform procedures to determine the validity or reliability of computer-based data. In general, electronic or computer data was not critical to satisfy the audit objective. KPMG conducted alternative procedures through interviews of application owners to determine the presence of PII data and the status of privacy initiatives. 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.

Methodology

In consultation with the FDIC OIG, we developed an audit approach based on our review of privacy legislative requirements and FDIC policies, procedures, and guidelines. The audit approach included the evaluation of a selection of internal control activities supporting compliance with legal requirements (Privacy Act, E-Government Act, Section 522, and OMB guidance). We considered risks, results of internal reviews, Government-wide and FDIC goals, the maturity of the privacy program, and other factors in making our selection. We evaluated the selected activities for a subset of collections of PII identified through review of FDIC business processes. We conducted interviews with appropriate FDIC personnel to obtain an understanding of each privacy control activity within the scope of the audit. Additionally, we reviewed FDIC documentation applicable to privacy, including FDIC directives, DIT internal policies, and the FDIC's *Privacy Program Strategic Framework* describing the FDIC's risk management framework and internal control activities. The *Results of Audit* section of this report presents the results of our review of these activities.

This audit did not assess controls at depository institutions, insured or regulated by the FDIC, that routinely provide financial information to the Corporation. We performed the audit at the FDIC's offices in Arlington, Virginia, from December 6, 2010 to June 30, 2011, and tested controls that were implemented as of May 10, 2011 for the six sampled collections of PII and two sampled SORNs. Throughout the audit, we met with FDIC management to discuss preliminary observations.

KPMG conducted this performance audit in accordance with 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 II – SIGNIFICANT CRITERIA

Applicable Statutory Privacy Criteria

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. Another requirement is that when collecting information from individuals, the agency is to include on the form a Privacy Act Statement which indicates the authority for soliciting the information, the intended purpose(s) and routine uses of the information, whether disclosure is required and the effect of not providing the information. 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.

Consolidated Appropriations Act of 2005, Division H, Section 522 (now 42 U.S.C. § 2000ee-2) 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 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.
- Preparing an annual report to Congress on the activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act, internal controls, and other relevant matters.

Section 522 also requires the Inspector General of each agency to periodically conduct a review of the agency's implementation of Section 522 requirements and report the results of its review to Congress. The Inspector General may contract with an independent, third party organization to conduct the review.

E-Government Act of 2002, Section 208. This Act seeks to promote electronic Government services and to enhance access to Government information consistent with laws regarding personal privacy. Section 208 is intended to protect personal information by requiring agencies to (1) conduct PIAs of information systems and collections and, in general, make PIAs publicly available; and (2) 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 also requires the Director, OMB, to draft guidelines regarding (1) agency posting of privacy policies on agency Web sites used by the public; and (2) translate privacy policies into a machine-readable format.

Applicable Privacy-Related OMB Guidance

OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. The Guidance provides detailed guidance to agencies on how to implement section 208 of the E-Government Act, see above. This memorandum provides definitions and explains when PIAs are or are not required, the manner in which PIAs are conducted, and their relationship with the Paperwork Reduction Act and the Privacy Act. The memorandum contains requirements for the agency Web site, specifically regarding privacy policies and persistent tracking technologies ("cookies"). Other provisions address privacy policies in machine-readable formats, responsibilities of agency officials, and reporting requirements. To the extent that the provisions of this memorandum are legally binding on the FDIC, the FDIC has taken steps to implement those provisions or has otherwise taken them into account. 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 Circular No. A-130, *Management of Federal Information Resources* . The circular establishes policy for the management of Federal information technology. The circular contains two relevant appendixes:

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.

Appendix III, *Security of Federal Automated Information Resources*, requires agencies to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. OMB A-130 Appendix III defines adequate security as security commensurate with the risk and magnitude of harm resulting from the loss; misuse; or unauthorized access to, or modification of, information. Most of the circular's provisions are legally binding on the FDIC.

The circular can be located at http://www.whitehouse.gov/omb/circulars/a130/a130trans4.pdf.

Applicable FDIC Policy regarding Privacy

FDIC Rules and Regulations. Parts 309 and 310, *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 by delineating the procedures that an individual must follow in exercising his or her access or amendment rights under the Privacy Act to records maintained by the Corporation in systems of record. FDIC Rules and Regulations Parts 309 and 310 can be located at:
http://www.fdic.gov/regulations/laws/rules/2000-3800.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.

FDIC Circular 1360.9, ***Protecting Sensitive Information,*** implements aspects of the Privacy Act and requires FDIC employees and contractors to follow the FDIC's "Procedures for Responding to Breach of Personally Identifiable Information."

FDIC Circular 1310.3, ***Information Technology Security Risk Management Program*****,** establishes guidance for managing risks to general support systems and sensitive applications and protecting the confidentiality, integrity, and availability of the sensitive data that the systems process.

FDIC RUP®, establishes standardized procedures covering the development lifecycle of FDIC application and IT systems. RUP® is a collected body of software engineering practices that are continually improved on a regular basis to reflect changes in industry practices.

DRR Circular 7100.2, *Maintenance and Protection of Bank Employee and Customer Personally Identifiable Information,* establishes DRR policies and guidelines for the protection and safeguarding of confidential and/or sensitive personally identifiable bank employee and customer information.

Other Relevant Privacy Guidance

The Government Accountability Office's ***Standards for Internal Control in the Federal Government*****,** November 1, 1999. The publication provides an overall framework for establishing and maintaining internal control and for identifying and addressing major performance management challenges and areas at great risk of fraud, waste, abuse and mismanagement. This publication builds upon prior internal control guidance from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This publication is relevant as it provides a broad framework to evaluate FDIC's Privacy Program. This document maybe found at (http://www.gao.gov/products/AIMD-00-21.3.1).

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

APPENDIX III – LIST OF ACRONYMS

Acronym	Definition
AICPA	American Institute of Certified Public Accountants
CAS	Claims Administration System
CIO	Chief Information Officer
CPO	Chief Privacy Officer
DIT	Division of Information Technology
DOLLARS	DRR Locations and Reporting System
DRR	Division of Resolutions and Receivership
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
GAGAS	Generally Accepted Government Auditing Standards
GAPP	Generally Accepted Privacy Principles
IIF	Information in an Identifiable Form
ISM	Information Security Manager
ISPS	Information Security and Privacy Staff
IT	Information Technology
KPMG	KPMG LLP
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POI	Persons of Interest
PTA	Privacy Threshold Analysis
RUP®	Rational Unified Process
Section 522	Section 522 of Division H of the Consolidation Appropriations Act of 2005, as amended
Section 208	Section 208 of the E-Government Act of 2002
SORN	System of Records Notice
SSN	Social Security Number
U.S.C.	United States Code

APPENDIX IV – GLOSSARY OF TERMS

Term	Definition
Information in Identifiable Form (IIF)	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, SSN, or other identifying code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements. OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, introduced the term PII as a replacement for IIF.
Information Security Managers (ISMs)	ISMs work together with FDIC security and privacy staff to educate employees and contractors who have access to corporate systems and data. ISMs are responsible for providing guidance to management officials regarding the Corporation's security mission, awareness, priorities and implementation approaches. They ensure the full implementation of the risk management program, including: assessing application security levels, preparing risk assessment reports, planning security requirements in new and enhanced systems, overseeing security plans and related Plans of Action and Milestones, and facilitating the successful completion of the certification and accreditation process. ISMs are also responsible for promoting awareness and compliance with FDIC security policies and procedures, legal mandates, accepted audit recommendations, and annual corporate and application-specific training.
Personally Identifiable Information (PII)	FDIC Circular 1360.9, *Protecting Sensitive Information*, which references OMB Memorandum M-06-19, defines PII as any information about an individual maintained by the FDIC that can be used to distinguish or trace that individual's identity, such as their full name, home address, email address (non-work), telephone numbers (non-work), 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 that is linked or linkable to an individual.
Structured Asset Sale Transaction	A structured asset sale transaction is the sale of a portfolio of assets owned by the FDIC or in its capacity as Receiver (i.e., the Seller). The transaction could involve the sale of any type of asset, but it usually involves owned real estate and/or commercial and multi-family non-performing mortgage loans. (Note, occasionally performing loans are included in the portfolio.) DRR coordinates the transaction from start to finish. DRR may secure a Financial Advisor who develops a plan to market the pool of assets and packages them in the most attractive form for investors.

Part II

Management's Comments and OIG Evaluation

MANAGEMENT'S COMMENTS AND OIG EVALUATION

On September 12, 2011, the FDIC's CIO, who also serves as the Director, DIT, and CPO, provided a written response to a draft of this report. The response is presented in its entirety beginning on the next page. Management concurred with KPMG's three recommendations, and the planned actions are sufficient to resolve all of them.

In response to the recommendations, DIT expects to finalize and issue corporate policy that includes a requirement for PIAs to be completed and publicly available before collecting, maintaining, and disseminating PII. DIT also plans to develop strategies for (1) elevating and reporting instances of non-compliance with privacy-related requirements to appropriate senior management officials who are in a position to ensure they are promptly and effectively resolved and (2) identifying and addressing instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA. DIT expects to complete these actions by December 30, 2011. A summary of management's response to the recommendations is on page II-4.

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

September 12, 2011

TO: Mark Mulholland
Assistant Inspector General for Audits

/**Signed**/
FROM: Russell G. Pittman
Chief Information Officer,
Director, Division of Information Technology, and
Chief Privacy Office

SUBJECT: Management Response to the Draft KPMG LLP Audit Report Entitled, *The FDIC's Privacy Program - 2011* (Assignment No. 2011-011)

This memorandum is in response to the subject draft Office of Inspector General (OIG) report, issued August 12, 2011, and performed by KPMG LLP. We appreciate and agree with the OIG/KPMG audit team's observations that the FDIC had properly:

- Appointed a Chief Privacy Officer (CPO) with overall responsibility for the FDIC's privacy program and submitted annual privacy reports to OMB and Congress as required by Section 522 in the Consolidated Appropriations Act of 2005;
- Established processes for preparing Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs) and making them publicly available
- Posted its privacy policies on the FDIC's public Web site consistent with Section 208 of the E-Government Act of 2002 and Privacy Act of 1974 requirements;
- Approved the two SORNs sampled, published them in the *Federal Register*, and addressed the content requirements of the Privacy Act; and further,
- Included the required legal disclosures, referred to as a Privacy Act Statement, on all sampled Division of Resolutions and Receiverships forms that collect Personally Identifiable Information (PII) from the public in accordance with the Privacy Act.

Based on the overall results of the audit, the Division of Information Technology (DIT) agrees with all three of the recommended steps to further strengthen FDIC's privacy program practices. This response outlines DIT's planned corrective actions for each of the recommendations.

.

Finding (1) Timeliness of PIAs

Recommendation (1)
Finalize and issue the draft corporate policy on PIA requirements and include clarifying language in the policy that requires PIAs to be completed and publicly available before collecting, maintaining, or disseminating PII.

Management Response (1) Concur.
The FDIC will finalize and issue the current draft FDIC Circular, *Implementation of the Privacy Provisions of the E-Government Act of 2002*, by December 30, 2011. The final policy will incorporate clarifying language that requires PIAs to be completed and publicly available before collecting, maintaining, or disseminating PII.

Recommendation (2)
Enhance privacy program controls by defining a strategy for elevating and reporting instances of non-compliance with relevant federal privacy requirements to appropriate senior management officials who are in a position to ensure they are promptly and effectively resolved.

Management Response (2) Concur.
Instances of non-compliance with relevant federal privacy requirements will be escalated to the Chief Information Security Officer (CISO) and/or Chief Privacy Officer (CPO) for action with the appropriate senior management. This strategy will be documented in an internal privacy program memorandum by December 30, 2011.

Finding (2) Content of PIAs

Recommendation (3)
Develop a strategy to help identify and address instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA.

Management Response (3) Concur.
FDIC's current draft circular, *Implementation of the Privacy Provisions of the E-Government Act of 2002*, will be updated to include a strategy to help identify and address instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA. The final policy will be issued by December 30, 2011.

Any questions regarding this response should be directed to Rack Campbell at (703) 516-1422.

cc: James H. Angel, Jr., Director OERM
Ned Goldberg, CISO and Deputy Director, DIT Information Security & Privacy
Steven B. Lott, Privacy Program Lead
Rack Campbell, Chief Audit and Internal Control

SUMMARY OF MANAGEMENT'S COMMENTS ON THE RECOMMENDATIONS

This table presents management's 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 finalize and issue the current draft circular, *Implementation of the Privacy Provisions of the E-Government Act of 2002*. The final policy will incorporate clarifying language that requires PIAs to be completed and publicly available before collecting, maintaining, or disseminating PII.	Dec. 30, 2011	N/A	Yes	Open
2.	Instances of noncompliance with relevant Federal privacy requirements will be escalated to the Chief Information Security Officer and/or CPO for action with the appropriate senior management. This strategy will be documented in an internal privacy program memorandum.	Dec. 30, 2011	N/A	Yes	Open
3.	The FDIC's current draft circular, *Implementation of the Privacy Provisions of the E-Government Act of* 2002, will be updated to include a strategy to help identify and address instances of new PII collections that occur outside of the traditional systems development life cycle that might require a PIA.	Dec. 30, 2011	N/A	Yes	Open

[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) the Office of Enterprise Risk Management 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.