Office of Inspector General

September 2006
Report No. 06-018

Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management

AUDIT REPORT

Office of Audits

OIG

Office of Audits

OIG

Background and Purpose of Audit

A number of federal statutes, policies, and guidelines are aimed at protecting the confidentiality, integrity, and availability of information in an identifiable form (IIF) from unauthorized use, access, disclosure, or sharing and protecting associated information systems from unauthorized access, modification, disruption, or destruction. Key federal statutes include the Privacy Act of 1974; section 208 of the E-Government Act of 2002; and section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, hereafter referred to as section 522.

The Federal Information Security Management Act of 2002 (FISMA) directs federal agencies to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluation to the Office of Management and Budget (OMB), the Comptroller General, and various congressional committees. On July 7, 2006, the OMB issued a memorandum entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. In response to OMB's request for privacy program information, the FDIC Office of Inspector General contracted with KPMG LLP (KPMG) to audit and report on the privacy management areas addressed in the OMB memorandum.

The objective of this audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy protection program. While KPMG did not evaluate the FDIC's privacy program as part of this audit, the report provides information on the program and related activities.

To view the full report, go to www.fdicig.gov/2006reports.asp

Report No. 06-018
September 2006

Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management

Results of Audit

KPMG reported that the FDIC has taken a number of actions to protect IIF since the passage of the Privacy Act of 1974 and continually enhance the corporate privacy protection program, policies, and procedures. Such recent actions include strengthening controls related to IIF and implementing mandatory Web-based privacy training to promote Privacy Act awareness among FDIC employees and contractor personnel. In addition, the FDIC has identified 46 systems containing IIF and performed required Privacy Impact Assessments (PIA) for most of those systems.

These actions were positive; however, the FDIC could further strengthen its privacy program by completing ongoing efforts to:

- monitor and enforce annual privacy awareness training requirements and formalize a privacy training program to ensure individuals in trusted roles receive job-specific training;
- implement measures to ensure 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; and
- establish and implement a formal plan of action and milestones to track privacy program deficiencies such as those identified in PIAs and required privacy reviews.

In addition, the Corporation should determine when it will submit an annual report to the Congress on its privacy protection activities, including complaints of privacy violations, internal controls, and other relevant matters as discussed in section 522.

Recommendations and Management Response

KPMG made no recommendations in the report. However, the Privacy Program Manager provided informal comments on a draft version of this report, which KPMG considered and incorporated into the report, as appropriate. Under contract with the OIG, KPMG will perform a more in-depth review, as required by section 522, of the FDIC's use of IIF and related privacy protection policy and procedures, and the firm will make appropriate recommendations, if necessary, at that time.

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

Office of Audits
Office of Inspector General

DATE: September 22, 2006

MEMORANDUM TO: Michael E. Bartell, Chief Privacy Officer

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

SUBJECT: KPMG LLP Report Entitled, *Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 06-018)

Attached is a copy of the subject report prepared by KPMG LLP (KPMG) under a contract with the Office of Inspector General. Please refer to the Executive Summary for the overall audit results.

The Chief Information Security Officer provided informal comments on a draft version of this report. KPMG has considered and incorporated the comments into the report, as appropriate.

If you have any questions concerning the report, please contact Stephen M. Beard, Deputy Assistant Inspector General for Audits, at (703) 562-6352, or Mark F. Mulholland, Director, Systems Management and Security Audits Directorate, at (703) 562-6316. We appreciate the courtesies extended to the audit staff.

Attachment

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

Response to Privacy Program Information Request in OMB's Fiscal Year 2006 Reporting Instructions for FISMA and Agency Privacy Management

Report Number 06-018

Prepared for the
Federal Deposit Insurance Corporation
Office of 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

CPO	Chief Privacy Officer
FDIC	Federal Deposit Insurance Corporation
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GAGAS	Generally Accepted Government Auditing Standards
IG	Inspector General
IIF	Information in an Identifiable Form
ISM	Information Security Manager
KPMG	KPMG LLP
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
SORN	System of Records Notice
SSN	Social Security Number

INTRODUCTION

On July 17, 2006, the Office of Management and Budget (OMB) issued Memorandum M-06-20 entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. In response to OMB's request for privacy program information, the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) contracted with KPMG LLP (KPMG) to conduct a performance audit and report on the privacy management areas addressed in Section D of the OMB memorandum. This is the second year that KPMG has supported the FDIC OIG in this audit work. KPMG conducted its performance audit in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States.

The objective of this audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy program. While KPMG did not evaluate the effectiveness of the FDIC's privacy program as part of this audit, this report provides information on the program and related activities. Reports on (1) the FDIC OIG responses to specific security-related questions in the referenced OMB memorandum and (2) the independent security evaluation required by the Federal Information Security Management Act of 2002 (FISMA), will be provided under separate cover.[1] Those two reports and this report are intended to fulfill the FDIC OIG's reporting responsibilities under FISMA and related OMB guidance. In addition, further information on the effectiveness of the FDIC's privacy program will be provided as part of the independent, third-party review required under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005, hereafter referred to as section 522. The FDIC OIG also contracted with KPMG to fulfill the review requirements of section 522.

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.

The FDIC's Privacy Program Manager provided informal comments in response to a draft of this report. KPMG considered and incorporated the comments, as appropriate, into the report. In general, the Privacy Program Manager agreed with KPMG's observations for strengthening the FDIC's privacy program.

[1] *Responses to Security-Related Questions in FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* (FDIC-OIG Report No. 06-019), dated September 2006; and *Independent Evaluation of the FDIC's Information Security Program* – 2006 (FDIC-OIG Report No. 06-022), dated September 2006.

BACKGROUND

The protection of sensitive information has never been more important or more threatened. The increasing use of computers to store and retrieve personal data about individuals has highlighted the government's duty to balance the necessity of maintaining information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy. In addition, recent high-profile incidents involving the potential compromise or loss of sensitive personal information further reinforce the need for federal agencies to implement measures to protect sensitive information entrusted to them.

A number of federal statutes, policies, and guidelines are aimed at protecting information in an identifiable form (IIF)[2] and associated information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, as discussed in Appendix II. One of the key policies is OMB Circular A-130, *Management of Federal Information Resources*, and its appendices.

RESULTS OF AUDIT

The FDIC has taken a number of actions to protect IIF since the passage of the Privacy Act of 1974 and continually enhanced the corporate privacy program, policies, and procedures. Such actions include strengthening controls related to IIF and implementing mandatory Web-based privacy training to promote Privacy Act awareness among corporate employees and contractor personnel. In addition, the FDIC has identified 46 systems containing IIF and completed required Privacy Impact Assessments (PIAs)[3] for 43 of those systems. These actions were positive; however, the FDIC could further strengthen its privacy program by completing ongoing efforts to:

- monitor and enforce annual privacy awareness training requirements and formalize a privacy training program to ensure individuals in trusted roles receive job-specific training;
- implement measures to ensure 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;

[2] OMB defines IIF as information in a system or 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.

[3] 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 Privacy Act requirements are considered when developing or procuring new or modified information technology that contains IIF.

- establish and implement a formal plan of action and milestones (POA&M) to track privacy management deficiencies such as those identified in PIAs and required privacy reviews; and
- submit an annual report to the Congress consistent with the provisions of section 522, addressing privacy protection activities, including complaints of privacy violations, internal controls, and other relevant matters.

KPMG is not making recommendations in this report. The FDIC OIG also contracted with KPMG to perform a privacy review, as required by section 522, of the FDIC's use of IIF and related FDIC privacy and data protection policies and procedures, and the firm will make appropriate recommendations, if necessary, at that time.

STATUS OF THE FDIC'S PRIVACY PROTECTION POLICIES AND PROCEDURES

The FDIC recognizes the need to take additional steps to implement a more effective privacy program. Since the 2005 OIG privacy evaluation,[4] the FDIC continues to develop and strengthen its privacy program, policies, and procedures. KPMG's review indicated that the FDIC has made progress by identifying computer applications processing IIF, establishing corporate privacy awareness training, conducting PIAs and required Privacy Act-related reviews, and satisfying records notification requirements. Key privacy initiatives, addressing areas in Section D of OMB Memorandum M-06-20, are detailed below.

Policies and Procedures. In accordance with section 522, the FDIC's Chief Privacy Officer (CPO) has primary responsibility for the Corporation's privacy protection policy and ensuring that IIF and related information systems are protected.

The FDIC's privacy program includes policies and procedures to manage and protect IIF. For example, the FDIC's PIA guide and template assist system owners in completing PIAs, if they are necessary based on the presence of IIF. Further, the FDIC has strengthened and revised its procedures related to the overall sensitivity of FDIC computer applications by using the Application Security Assessment,[5] which includes questions to aid identifying any IIF in an application. During FY 2006, the FDIC identified applications containing IIF and developed a phased approach for performing PIAs. As of September 20, 2006, the FDIC had completed PIAs for 43 out of 46 applications identified as containing IIF. In addition, the FDIC made

[4] *Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management* (FDIC-OIG Report No. 05-033), dated September 16, 2005.
[5] The FDIC previously used the Sensitivity Assessment Questionnaire to determine the overall sensitivity of an FDIC system or application. Certain responses generate specific security control recommendations, including the necessity to complete a PIA.

sanitized versions of all but one[6] of the completed PIAs publicly available on the FDIC's Privacy Program Web site in accordance with the E-Government Act of 2002 requirements. Furthermore, in response to OMB's Memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, the FDIC is drafting a policy that requires encryption of production data stored at a remote location, authorization for the duplication of IIF information, and disposal of any copies of privacy information within 90 days of the duplication. The FDIC has also acted to ensure its remote authentication and "time-out" functions meet OMB requirements.

Awareness and Training. In October 2005, the FDIC implemented corporate-wide privacy awareness training that included coverage of privacy laws, regulations, and policies. The completion of this Web-based course is mandatory for all FDIC employees and contractors. The FDIC tracks training completion using a security awareness and training database. However, the FDIC could strengthen monitoring and enforcing compliance with the privacy awareness training requirements. During the 12 months ended June 2006, the FDIC had created 983 new user (employee and contractor) accounts. KPMG sampled 45 such user accounts and found that 9 of those users had not completed the required privacy awareness training. The FDIC attributed the lack of compliance to a delay between the privacy awareness training completion deadline[7] and the time divisional Information Security Managers (ISM) could access privacy training compliance reports to perform necessary follow-up. The FDIC is addressing this issue, and ISMs have been reminded to comply with the awareness training requirement.

In addition, the FDIC provides one-on-one or team-specific privacy training on an ad-hoc basis. However, this type of training has not been incorporated into a formal privacy training program. The Privacy Program Manager indicated that the Corporation has undertaken an initiative with the Corporate University to provide specific privacy training. A formal job-specific training program would help to ensure that FDIC personnel and contractors directly involved in administering IIF or information systems processing IIF are familiar with information privacy laws and regulations applicable to their specific job duties and responsibilities and help prevent inappropriate access and disclosure.

Privacy Reviews. The FDIC has completed all reviews of FDIC compliance with various provisions of the Privacy Act as required by OMB Circular A-130, Appendix 1, *Federal Agency Responsibilities for Maintaining Records About Individuals.*[8] These reviews focus

[6] A waiver from the public posting requirement was requested for one system due to the sensitivity of the data in the system, as well as business needs to ensure confidentiality of the system. Such a waiver was consistent with the E-Government Act and OMB's implementing guidance.

[7] The privacy training was announced by global e-mail on October 11, 2005 and included a mandatory completion date of October 28, 2005.

[8] OMB Circular A-130, Appendix I, requires agencies to conduct reviews of the following topics, at the indicated frequency: Section (m) Contract, Recordkeeping Practices, Privacy Act Training, Violations, and System of Records Notices every 2 years; Routine Use Disclosures and Exemption of System of Records reviews every 4 years; and Matching Programs annually.

attention on particular Privacy Act requirements as indicated by the following examples from the circular:

- **Recordkeeping Practices.** Biennially review agency recordkeeping and disposal policies and practices in order to assure compliance with the Privacy Act, paying particular attention to the maintenance of automated records.
- **Privacy Act Training.** Biennially review agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, the agency's implementing regulation, and any special requirements of their specific jobs.

Privacy Impact Assessments and Notice Requirements. The FDIC has made significant progress in identifying systems containing IIF. For example, the FDIC completed an initial exercise in September 2005 to identify computer applications with Social Security number (SSN) information. Following the completion of this exercise, the FDIC conducted another review to identify systems with any additional IIF data. The FDIC identified 46 applications containing IIF and developed a phased approach for performing the associated PIAs. As of September 20, 2006, the FDIC had completed PIAs for 43 of these applications. The PIAs for the remaining three applications containing IIF are scheduled for completion by December 31, 2006. Additionally, the FDIC has published 24 System of Records[9] Notices (SORN) on the FDIC Web site and in the *Federal Register*, as required by the Privacy Act, and is proposing 4 new FDIC Privacy Act SORNs to replace the outdated Unofficial Personnel Records notice.[10] The SORNs help to ensure that information about FDIC maintenance and use of records containing IIF is publicly disclosed. The FDIC has also included its privacy policies on its public-facing Web site in furtherance of its disclosure activities.

Persistent Tracking. The FDIC continues to annually review the use of persistent tracking technologies, also known as Web site cookies. There are two types of Web site cookies, session and persistent cookies. Session cookies are temporary and are erased when a user closes the Web browser, whereas persistent cookies remain on a user's computer until the user erases them. The FDIC uses persistent cookies only as part of the Statistics on Depository Institutions application. The FDIC has properly obtained agency-head approval to collect this information and informs visitors of its use. Additionally, the FDIC posts Privacy Notices on all public Web sites and on any Web page where the FDIC uses session cookies to collect information consistent with OMB guidance.[11]

[9] The Privacy Act of 1974 states, "The term system of records means 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."

[10] The Web site contains only the name of the system and indicates that it is to be revised at a later time.

[11] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003, indicates that where there is a compelling need to use persistent tracking technology, the agency must post clear notice of its privacy policy.

Internal Oversight. In addition to performing the privacy reviews discussed earlier to comply with requirements in OMB Circular A-130, Appendix I, the FDIC conducts internal reviews of compliance with information privacy laws and regulations. For example, in November 2005, the FDIC conducted a review of several published directives that contain privacy references and added or revised content, language, and references, as necessary. Continuing these reviews will help the FDIC to ensure compliance with current privacy requirements, such as OMB's memorandum M-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, which emphasized critical safeguards for protecting privacy information on mobile computers and devices. The memorandum requires an agency review of these safeguards.

The FDIC needs to implement measures that would provide assurance that the 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 and discussed in OMB Memorandum M-06-20. The need for continuous auditing of systems security controls was also identified in the FY 2006 independent evaluation of the FDIC's security program.[12] The Privacy Program Manager indicated that a DIT project team is evaluating technologies to provide continuous monitoring. Continuous monitoring of compliance controls will provide the FDIC with ongoing awareness and periodic compliance metrics regarding the collection, use, and distribution of IIF. Additionally, the FDIC needs to complete a comprehensive and formal POA&M to track privacy program compliance deficiencies. The Privacy Program Manager indicated that corrective actions related to audits would be tracked through the corporate audit finding tracking system and non-audit related initiatives through the established Privacy Program monthly status report. However, the Privacy Program monthly status report was not always completed and did not consistently include required resources or track items through completion. A formal POA&M for the privacy program will enhance the FDIC's ability to identify, assess, prioritize, and monitor the progress of corrective efforts for identified privacy weaknesses, including those contained in PIAs and privacy reviews.

The FDIC has determined that the Corporation needs to report annually to Congress regarding activities affecting privacy as required by section 522. The FDIC Privacy Program Manager indicated the FDIC plans to comply with this requirement by submitting such a report in FY 2006. KPMG intends to follow up in the upcoming section 522 compliance audit to determine the status on the FDIC's preparation of this report.

OIG Coordination. The FDIC coordinated with the OIG on privacy program oversight by providing the OIG with a compilation of FDIC privacy and data protection policies and procedures, a summary of the FDIC use of IIF, and verification of the intent to comply with both federal and corporate agency policies and procedures. Section 522 required the FDIC to provide a report containing this information to the Inspector General; the report was received on September 15, 2005.

[12] In the FY 2006 *Independent Evaluation of the FDIC's Information Security Program*, (FDIC-OIG Report No. 06-22), dated September 2006, the OIG suggested that the FDIC complete its security risk management methodology to define procedures for performing continuous monitoring of system security controls after system accreditation.

KPMG is making no recommendations in this report. The FDIC OIG has contracted with KPMG to perform a privacy review, designed to meet the various requirements of section 522, of the FDIC's use of IIF and related privacy protection policy and procedures, and the firm will make appropriate recommendations, if necessary, at that time.

APPENDIX I

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of KPMG's performance audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy program. The audit focused on privacy program areas addressed in Section D of OMB's July 17, 2006 memorandum M-06-20 entitled, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* As part of the audit work, KPMG reviewed prior OIG reports (listed below) related to privacy. The results of this audit support the OIG in fulfilling its evaluation and reporting responsibilities under FISMA and M-06-20.

To accomplish the objective, KPMG relied on information-gathering techniques such as interviewing key FDIC officials with privacy responsibilities; reviewing relevant FDIC policies, procedures, and documentation; and performing other appropriate audit procedures. Also, KPMG considered the results from the following OIG reports but did not follow up on the recommendations in those reports. Such follow-up will be performed as part of the required review under section 522.

- FDIC OIG Report No. 05-033, *Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management*, dated September 16, 2005. The objective of the audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy management program. The results of the audit indicated that while the FDIC had taken a number of actions to protect IIF, the FDIC needed to complete several ongoing efforts to strengthen its privacy program. Such efforts included, among other things, the identification of all FDIC-maintained IIF and the establishment of a corporate-wide privacy training and education program.

- FDIC OIG Report No. 06-005, *FDIC Safeguards Over Personal Employee Information*, dated January 6, 2006. The objective of the evaluation was to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form. Based on the results of the evaluation, the FDIC OIG noted the FDIC made efforts to enhance its established privacy program in response to legislative requirements and breaches of FDIC employee information. However, the FDIC OIG issued 15 recommendations to help ensure the FDIC complies fully with privacy-related legislation and regulations; identifies personal employee information maintained by the FDIC and its contractors that needs to be protected; and implements sufficient administrative, physical, and technical controls over such information.

- FDIC OIG Report No. 06-016, *Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc.*, dated June 29, 2006. The objective of the audit was to determine whether the FDIC has adequate controls for ensuring the secure disposal of sensitive information by Iron Mountain for the FDIC's headquarters offices. The results of the audit indicated the FDIC established a number of key controls to ensure the secure disposal of sensitive information by Iron Mountain. However, the

FDIC OIG attributed insufficient contract oversight to several inconsistencies with established policy, procedures, and contractual language and issued a total of four recommendations.

- FDIC OIG Report No. 06-017, *DRR's Protection of Bank Employee and Customer Personally Identifiable Information*, dated September 15, 2006. The objective of the audit was to determine whether DRR adequately protects IIF collected in hardcopy form that is maintained as a result of resolution and receivership functions. The FDIC OIG reported that the division had not established a Records Management Program that defines recordkeeping requirements for the inventory, maintenance, control, and use of hardcopy documents.

KPMG did not separately perform procedures to review program performance measures, assess the FDIC's compliance with laws and regulations, evaluate the FDIC's internal control, or determine that computer-based data were valid and reliable. In addition, KPMG did not design specific audit procedures to detect fraud; however, throughout the audit, KPMG and the OIG were sensitive to the potential for fraud, waste, abuse, and mismanagement. KPMG performed the audit at the FDIC's offices in Arlington, Virginia, during the period June through August 2006 in accordance with GAGAS issued by the Comptroller General of the United States.

APPENDIX II

PRIVACY-RELATED LAWS, POLICIES, AND GUIDELINES

A number of federal statutes, 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 on 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 of these requirements is to publish notices in the *Federal Register* that include information such as the categories of records maintained in the agency systems, the routine uses of the records, and the manner in which individuals may access the information. As a federal agency, the FDIC is subject to the requirements of the Act.

- **The E-Government Act of 2002, section 208,** requires agencies to (1) conduct PIAs of information technology 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 section 208 applies to the Corporation.

- **Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005** requires, among other things, that agencies protect IIF, designate a CPO, conduct PIAs under appropriate circumstances, report to the Congress and agency IG on privacy matters, and provide training to employees on privacy and data protection policies. Section 522 also requires that every 2 years, the agency IG contract with an independent third party to conduct a review of the agency's privacy program and practices and that the IG issue a report based on that review. Agencies must establish comprehensive privacy and data protection procedures by December 2005. The FDIC has determined that section 522 applies to the FDIC.

- **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.

- **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 provision of the E-Government Act of 2002. The guidance directs agencies to

conduct reviews of how information about individuals is handled within their agencies when they use information technology to collect new information, or when agencies develop or buy new information technology systems to handle collections of PII. The FDIC has taken steps to implement this memorandum.

- **OMB Memorandum M-05-08*, Designation of Senior Agency Officials for Privacy***, contains OMB's request that each executive department and agency identify to OMB the senior official who has the overall agency-wide responsibility for information privacy issues. The FDIC complied with this request by designating the FDIC Chief Information Officer as the Senior Official for Privacy.

- **OMB Memorandum M-06-15*, Safeguarding Personally Identifiable Information***, describes responsibilities under law and policy to appropriately safeguard sensitive PII and training employees on their responsibilities in this area. OMB requires the senior official for privacy to conduct a review of policies and processes and take corrective action as appropriate to ensure adequate safeguards to prevent misuse or unauthorized access to PII. Any weaknesses found are to be identified in security POA&Ms already required by FISMA. Although the level of legal applicability of this memorandum has not been determined, the FDIC has taken steps to implement its provisions.

- **OMB Memorandum M-06-16*, Protection of Sensitive Agency Information***, requires departments and agencies to take specific actions to provide for the protection of sensitive information. Requirements include 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 holding sensitive information. Although the level of legal applicability of this memorandum has not been determined, the FDIC has taken steps to implement its provisions.

- **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 to the questions, 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 PII. 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 that are missing from the agency's inventory of major information systems.

- **Homeland Security Presidential Directive (Hspd)-12,** the ***Policy for a Common Identification Standard for Federal Employees and Contractors***. Hspd-12 requires agencies to be in compliance with a standard architecture for a common identification

standard for federal employees and contractors by November 2006. The FDIC is not legally bound by this requirement but intends to follow it.

- **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 and Technology IT Policy Memorandum, January 24, 2001, *Cookies in Internet Products,*** establishes the policy and standard for use of cookies in Internet, FDICnet, and extranet-type products developed or deployed by FDIC.