Office of Inspector General

September 2005
Report No. 05-033

Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management

AUDIT REPORT

Office of Audits

OIG

Office of Audits

Report No. 05-033
September 2005

Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management

Background and Purpose of Audit

A number of federal statutes, policies, and guidelines are aimed at protecting information in an identifiable form 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.

This audit was conducted in response to a request for privacy program information contained in the Office of Management and Budget's (OMB) June 13, 2005 memorandum entitled, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

The objective of the audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy management program.

To view the full report, go to www.fdicig.gov/2005reports.asp

Results of Audit

The FDIC has taken a number of actions to protect information in an identifiable form (IIF) since the passage of the Privacy Act of 1974. Such actions include establishing corporate policies and procedures to safeguard IIF, identifying corporate Privacy Act systems of record that contain IIF and publishing related notices in the *Federal Register*, and posting a privacy statement on the FDIC's public Web site. Additionally, control improvements were underway at the time of our audit. These included appointing a Chief Privacy Officer and Privacy Program Manager to oversee and implement the Corporation's privacy program and implementing a privacy Web site to promote awareness among employees and contractor personnel regarding privacy requirements, policies, and practices. In addition, the FDIC strengthened controls over IIF in hardcopy format by providing additional shredding bins throughout its headquarters offices to securely dispose of sensitive data.

The above actions were positive; however, the FDIC needed to complete a number of ongoing initiatives to ensure adequate protection of employee IIF and compliance with federal privacy-related statutes, policies, and guidelines. Specifically, the FDIC needed to complete ongoing efforts to:

- identify all FDIC-maintained IIF and take appropriate actions to ensure this information is properly protected;
- review privacy policies and procedures to ensure they are current, comprehensive, and complete; and
- implement a corporate-wide training and education program, including job-specific training where appropriate.

The FDIC also needed to execute contractor confidentiality agreements as prescribed by FDIC policy.

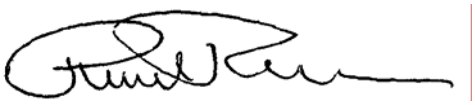
We made no recommendations in this report because the FDIC is taking steps to establish a comprehensive privacy program.

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434

Office of Audits
Office of Inspector General

DATE: September 16, 2005

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



FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management*
(Report No. 05-033)

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) has completed an audit of the status of the FDIC's privacy program and related activities. This audit was conducted in response to a request for privacy program information contained in the Office of Management and Budget's (OMB) June 13, 2005 memorandum entitled, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.* We are providing the results of this audit to you in your capacity as the FDIC's Chief Privacy Officer (CPO). The objective of the audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy management program. We are providing you our responses to specific security-related questions in the referenced OMB memorandum, along with our independent security evaluation report required by the Federal Information Security Management Act of 2002 (FISMA) under separate cover.[1]

BACKGROUND

A number of federal statutes, policies, and guidelines are aimed at protecting information in an identifiable form (IIF)[2] from unauthorized use, access, disclosure, or sharing and associated information systems from unauthorized access, modification, disruption, or destruction. A brief description of key privacy-related statutes, policies, and guidelines and their applicability to the FDIC follows.

---

[1] *Responses to Security-Related Questions Raised in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management* (Report No. 05-034), dated September 16, 2005; and *Independent Evaluation of the FDIC's Information Security Program-2005* (Report No. 05-040), scheduled for issuance on September 30, 2005.

[2] OMB defines "information in an identifiable form" 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.

- **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 for this purpose, the FDIC is subject to the requirements of the Act.
- **The E-Government Act of 2002, section 208,** requires agencies to (1) conduct privacy impact assessments (PIA) of information systems and collections and, in general, make PIAs publicly available; (2) post privacy policies on agency Web sites used by the public; (3) translate privacy policies into a machine-readable format; and (4) report annually to the OMB on compliance with section 208. The FDIC has determined that section 208 applies to the Corporation.
- **Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005**[3] 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 Corporation.
- **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 and has designated a senior agency official for privacy as discussed below. Subsequent OMB policy[4] 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.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of the audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy management program. To accomplish our objective, we relied on professional services provided by KPMG LLP (KPMG). KPMG's work included interviewing key FDIC officials with privacy responsibilities; reviewing relevant FDIC policies, procedures and documentation; and performing other appropriate audit procedures. As part of our oversight of

[3] This Act is division H of the Consolidated Appropriations Act, 2005, Public Law No. 108-447.

[4] Such policy includes OMB Memorandums M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, and M-05-08, *Designation of Senior Agency Officials for Privacy*.

KPMG, we evaluated the nature, timing, and extent of work described in its evaluation program, obtained an understanding of KPMG's methodologies and assumptions, attended key meetings, monitored progress throughout the evaluation, and performed other procedures we deemed necessary. In this manner, we were assured that KPMG's work complied with generally accepted government auditing standards (GAGAS).

The limited nature of our work did not require that we separately perform procedures to review program performance measures, assess the FDIC's compliance with laws and regulations, evaluate the FDIC's internal control, or assure ourselves that computer-based data were valid and reliable. In addition, we did not design specific audit procedures to detect fraud; however, throughout our work, we were sensitive to the potential for fraud, waste, abuse, and mismanagement. We performed our work at the FDIC's headquarters offices in Washington, D.C., and Arlington, Virginia, during the period July through August 2005. On September 14, 2005, the FDIC Privacy Program Manager provided updated information regarding progress on the FDIC's privacy program, which we included in the report. We conducted our work in accordance with GAGAS.

STATUS OF THE FDIC'S PRIVACY PROGRAM AND PRACTICES

The FDIC has taken a number of actions to protect IIF since the passage of the Privacy Act of 1974. Such actions include establishing corporate policies and procedures to safeguard IIF, identifying corporate Privacy Act systems of record that contain IIF and publishing related system of record notices in the *Federal Register*, and posting a privacy statement on the FDIC's public Web site. In addition, the OIG has conducted reviews of, and reported on, the FDIC's privacy program practices in recent years.[5] These reviews have focused on the FDIC's efforts to safeguard employee IIF; control the use of SSN information for non-employees (such as depositors, debtors, and loan guarantors); and ensure the adequacy of privacy and security disclosure statements on the Corporation's Web sites. Generally, these reviews concluded that the FDIC had taken measures to safeguard IIF, but that important control improvements were needed. Finally, the OIG performed an annual independent evaluation of the FDIC's information security program as required by FISMA that included determining whether the FDIC had implemented controls that maintain appropriate confidentiality of information resources.

The FDIC has taken recent action to strengthen its privacy program and practices, and additional control improvements were underway at the time of our audit. In March 2005, in response to passage of section 522, the FDIC appointed a senior official, the Director, Division of Information Technology (DIT), as the FDIC's CPO with overall responsibility for the Corporation's privacy program. The Director was also designated as the senior agency official for privacy in accordance with OMB policy. The FDIC also designated a Privacy Program Manager in April 2005 to support the CPO in developing and implementing corporate privacy requirements. In addition, the FDIC implemented a privacy Web site to promote awareness among FDIC employees and contractor personnel regarding privacy requirements, policies, and practices. In September 2005, a public Web

[5] Reports entitled, *FDIC's Privacy and Security Notices-Requirements and Policy Statements on the Internet and Intranet*, dated May 19, 2000 (Report No. 00-004); *FDIC's Information Handling Practices for Sensitive Employee Data*, dated October 11, 2000 (Report No. 00-006); and *Control Over the Use and Protection of Social Security Numbers by Federal Agencies*, dated February 14, 2003 (Report No. 03-012).

site was launched to provide information regarding the Privacy Act and privacy policies of the FDIC. The Web site includes information about employee responsibilities, disclosure procedures, privacy program contacts, and PIAs. Further, the FDIC strengthened controls over IIF in hardcopy format by providing additional shredding bins throughout its headquarters offices to securely dispose of sensitive data. These actions were positive; however, the FDIC needed to complete a number of ongoing initiatives to ensure adequate protection of employee IIF and compliance with federal privacy-related statutes, policies, and guidelines. A brief summary of the FDIC's key privacy initiatives follows.

- **Identifying FDIC-maintained IIF.** DIT personnel performed a preliminary assessment of the FDIC's major information systems during our audit to determine which systems process SSNs. Based on the results of the assessment, DIT will determine whether controls in the major information systems sufficiently protect employee SSNs and will take any needed corrective action. In addition, DIT, together with the FDIC's divisions and offices, recently initiated a corporate effort to identify SSNs maintained in electronic and hardcopy format outside of the FDIC's major information systems. Such SSN data may be stored or processed by organizational units in locally maintained systems, databases, spreadsheets, and documentation. Following the completion of this corporate-wide analysis, the FDIC plans to take appropriate steps to ensure that all FDIC-maintained SSN data is adequately protected.

- **Policies and Procedures.** In December 2004, the FDIC modified its *Standard Operating Procedures for Processing Sensitivity Assessment Questionnaires* to include privacy considerations. The FDIC plans to apply these revised procedures to all of its applications over the next several years. The FDIC also developed a PIA guide and template for preparing PIAs in July 2005. At the time of our audit, the FDIC had completed a PIA on only 1 (the Corporate Human Resources Information System) of the 26 information systems that DIT had identified as containing SSNs and was working to complete PIAs on the remaining information systems. The Privacy Program Manager advised us that PIAs had been completed on 25 of 26 information systems as of September 14, 2005 and that the FDIC was working to complete a PIA on the remaining information system. The FDIC may need to complete or amend and publish, as necessary, PIAs or Privacy Act based on the results of its efforts to identify SSNs maintained throughout the Corporation. Additionally, according to the Privacy Program Manager, the CIO Council is reviewing a proposed modification to its charter to add a privacy advisory role to provide a forum for privacy issues. The FDIC is continuing to review its privacy policies and procedures to ensure they are current, comprehensive, and complete. Where additional or revised procedures are needed, the FDIC plans to take appropriate corrective action.

- **Training.** The FDIC is working to develop a corporate-wide training and education program to increase employee and contractor awareness of their responsibilities regarding the protection of IIF. To comply with federal privacy policy, the FDIC will need to provide individuals in trusted roles with job-specific training. According to the Privacy Program Manager, privacy training was held for members of the CIO Council on September 6, 2005. Privacy training is planned for members of the Operating Committee in October 2005. Also, the FDIC plans to begin mandatory privacy training for all employees and contractors

during the week of September 19, 2005. Finally, FDIC information security managers for three major information systems stated that they were modifying their application-specific security training to address privacy.

- **Privacy Reviews and Evaluations.** The FDIC's Privacy Program Manager stated that the FDIC had reviewed its corporate documentation and contracts in the prior fiscal year as required by OMB Circular No. A-130, Appendix I. These reviews included determining compliance with specific provisions of the Privacy Act of 1974. However, during our audit, the FDIC was in the process of documenting the results of these reviews. Subsequent to our fieldwork, the Privacy Program Manager informed us that these reviews had been completed and documented. In addition, section 522 requires the FDIC to prepare several reports and reviews. For example, the CPO must conduct PIAs of systems containing IIF and prepare a report to the Congress annually on the activities that affect privacy. Also, a written report of the FDIC's use of IIF along with its privacy and data protection policies and procedures is required to be recorded with the IG to serve as a benchmark for the agency. Finally, section 522 requires the FDIC to perform an independent third-party review of the privacy and data protection procedures of the agency. This review will be performed through the OIG and includes, among other things, ensuring that all technologies for collecting, using, storing, and disclosing information allow for continuous auditing of compliance with privacy policies and practices.

As reported in our independent security evaluation required by FISMA, FDIC contractor personnel were not routinely executing confidentiality agreements as prescribed by FDIC contracting policy and information technology (IT) service contracts. The FDIC's standard IT service contract language requires contractors, subcontractors, and their employees to sign confidentiality agreements. Confidentiality agreements are designed to hold contractor personnel accountable for maintaining the confidentiality of FDIC information, data, and systems provided under a contract. We found that oversight managers and contract specialists generally were not obtaining the agreements from the contractor and contract personnel.

Privacy has been and continues to be of significant concern to the public and the Congress. Recent reports of unauthorized disclosure of IIF in the financial services industry, as well as a recent report of unauthorized access to IIF on a large number of current and former FDIC employees, highlight the criticality of an effective and comprehensive privacy management program. The OIG will continue to work with the Corporation throughout the coming year to ensure that appropriate privacy controls are in place to safeguard all the FDIC's IIF. We made no recommendations in this report because the FDIC is taking steps to establish a comprehensive privacy program.