Office of Inspector General

January 2006
Report No. 06-005

FDIC Safeguards Over Personal Employee Information

EVALUATION REPORT

Office of Audits

oig

Office of Audits

OIG

Background and Purpose of Evaluation

The Federal Trade Commission defines identity theft as "a fraud that is committed or attempted, using a person's identifying information without permission." Identity theft is one of the fastest growing crimes in the country and has involved private sector and federal agency information.

The FDIC is no exception and has experienced several breaches involving personal employee information. For example, a security breach identified in 2005 involved unauthorized access to personal information for a large number of current and former FDIC employees.

Among other things, the Privacy Act of 1974 requires federal agencies to limit the collection, disclosure, and use of personal information maintained in systems of records and to establish reasonable safeguards over those records.

In July 2005, the Director, Division of Administration (DOA), requested that we perform an evaluation of this area. Our objective was to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form.

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

Report No. 06-005
January 2006

FDIC Safeguards Over Personal Employee Information

Results of Evaluation

The FDIC has a corporate-wide program for protecting personal employee information, has appointed a Chief Privacy Officer (CPO) with responsibility for privacy and data protection policy, and is making efforts to enhance its privacy program in response to legislative requirements and breaches of FDIC employee information. The following table presents programmatic initiatives and notable physical and electronic safeguards over personal employee information that the FDIC has in place or underway.

	Initiatives In Place or Underway
Privacy Program	• The Legal Division is updating required system of records notices (SORN). • The Legal Division documented required privacy reviews. • The CPO developed a Privacy Web site. • The CPO has developed and implemented privacy awareness training courses.
Physical Safeguards	• Human Resources Branch (HRB) operations and files containing Social Security Numbers (SSNs) are housed in limited-access, secured office space. • HRB employees are required to encrypt all internal and external transmissions containing sensitive information. • HRB has eliminated SSNs from most standard reports, including staffing tables. • Records Management has eliminated SSNs from most FDIC forms. • HRB has installed personal shredders for all HRB staff, and the Corporation has installed secured shredding bins in all FDIC Headquarters offices.
Electronic Safeguards	• The Division of Information Technology (DIT) completed required information security procedures for the FDIC's human resources and accounting systems. • DIT conducted a review of FDIC applications to identify those containing SSNs. • DIT conducted a corporate-wide survey to collect information about electronic and hardcopy sources of data containing SSNs. • DIT completed Privacy Impact Assessments for 27 systems containing SSNs. • DOA and the Division of Finance (DOF) have reviewed user access levels for the FDIC's human resources and accounting systems. • FDIC human resources and accounting systems use employee identification numbers instead of SSNs.

Source: OIG Analysis.

We identified opportunities for the FDIC to strengthen its privacy program for protecting personal employee information, including:

- Developing an overarching privacy policy to ensure coordination between the CPO and Privacy Act Clearance Officer and updating SORNs pertaining to employee information, especially information maintained by contractors.
- Ensuring that contracts, for which the scope requires contractors to maintain personal employee information, contain adequate references to the Privacy Act, appropriate confidentiality clauses, and signed confidentiality agreements.
- Conducting some form of security review or obtaining assurances through third-party security reviews for contractors and vendors that maintain personal employee information in electronic form.

These additional controls will help to ensure that 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.

Recommendations and Management Response

We made 15 recommendations to strengthen the FDIC's privacy program. The Corporation generally concurred with our report and agreed to take corrective action on 12 recommendations. The FDIC indicated, and we concur, that actions taken and/or controls in place were sufficient to address the remaining three recommendations.

TABLE OF CONTENTS

Acronyms

AICPA	American Institute of Certified Public Accountants
AO	Administrative Officer
APM	Acquisition Policy Manual
ARMS	Automated Records Management System
ASB	Acquisition Services Branch
BAS	Benefits Allocation System
CDSSC	Corporate Data Sharing Steering Committee
CHRIS	Corporate Human Resources Information System
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
CO	Contracting Officer
COTS	Commercial-off-the-Shelf
CPO	Chief Privacy Officer
CTAW	Corporate Time and Attendance Worksheet
CU	Corporate University
CWG	Collaborative Working Group
DIT	Division of Information Technology
DMB	Delivery Management Branch
DOA	Division of Administration
DOF	Division of Finance
DOI	Division of Insurance
DSC	Division of Supervision and Consumer Protection
EAB	Enterprise Architecture Board
EIN	Employee Identification Number
ETVPS	Electronic Travel Voucher Processing System
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
HRB	Human Resources Branch
IRS	Internal Revenue Service
ISS	Information Security Staff
IT	Information Technology
NFC	National Finance Center
NFE	New Financial Environment
NPRC	National Public Records Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPF	Official Personnel Folder
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
RMS	Rights Management Services

SMS	Security Management Section
SORN	System of Records Notice
SOW	Statement of Work
SSN	Social Security Number
T&A	Time and Attendance
TIN	Tax Identification Number
UPF	Unofficial Personnel File
UPS	Unofficial Personnel System

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

Office of Audits
Office of Inspector General

DATE: January 6, 2006

MEMORANDUM TO: Douglas H. Jones
Acting General Counsel

Michael E. Bartell,
Chief Information Officer and
Director, Division of Information Technology

Arleas Upton Kea
Director, Division of Administration

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

SUBJECT: *FDIC Safeguards Over Personal Employee Information*
(Report No. 06-005)

In response to a security breach involving unauthorized access to personal employee information on a large number of current and former FDIC employees, the Director, Division of Administration (DOA) requested that we evaluate the FDIC's safeguards over personal employee information. For purposes of this review, we defined personal employee information to be information in an identifiable form, including an employee's name, home address, and social security number (SSN).[1] We focused our work on safeguards over SSNs because the security breach involved the unauthorized access and misuse of SSNs. The objective of our review was to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form. Additional details on our objective, scope, and methodology are provided in Appendix I of this report.

BACKGROUND

The Federal Trade Commission (FTC) defines identity theft as "a fraud that is committed or attempted, using a person's identifying information without permission." Between January and December 2004, Consumer Sentinel, the complaint database developed and maintained by the FTC, received over 635,000 consumer fraud and identity theft complaints. Consumers reported losses from fraud of more than $547 million.

In March 2005, the Office of Inspector General (OIG) notified the FDIC that a small number of current and former FDIC employees were apparent victims of fraud. In June 2005, the FDIC became aware that as a result of the apparent fraud, personal employee information for all FDIC employees in an official pay status as of July 2002 had been compromised. The FDIC promptly notified all current and former employees in pay status as of July 2002 of the compromise.

[1] The Office of Management and Budget (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, 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 is the primary statute that regulates the federal government's uses of personal information. The Privacy Act has been augmented by a number of other laws and regulations, including the E-Government Act of 2002, Section 208(e); the Federal Information Security Management Act of 2002 (FISMA); Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005[2] (referred to as Section 522 for purposes of this report); and OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals* (OMB Circular A-130, Appendix I). These laws and regulations have required government agencies to enhance and report on their privacy programs. Appendix II lists and describes the laws and regulations applicable to privacy.

The FDIC has had a privacy program since the inception of the Privacy Act. The FDIC Legal Division's Freedom of Information Act-Privacy Act Group (FOIA-PA Group) has responsibility for corporate-wide compliance with the Privacy Act. Under the Privacy Act, the FDIC is responsible for:

- Maintaining in its systems of records[3] only such information necessary and relevant to a function that the Corporation is required to perform either by statute or by executive order of the President.
- Ensuring that no records are maintained describing how an individual exercises rights guaranteed by the First Amendment.
- Preparing and publishing a public notice of the establishment or revision of a system of records in the *Federal Register*, known as a System of Records Notice (SORN).
- Supplying a "Privacy Act Notice" to each individual from whom the Corporation collects information that informs the individual of the authority for the solicitation of information; whether disclosure of the information is mandatory or voluntary; the principal purposes for which the information will be used; the routine uses to be made of the information; and the effects, if any, of not supplying all or part of the information.
- Establishing reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access.
- Ensuring that all records maintained are accurate, relevant, timely, and complete.

EVALUATION RESULTS

The FDIC has a corporate-wide program for protecting personal employee information, has appointed a Chief Privacy Officer (CPO) with responsibility for privacy and data protection policy, and is making efforts to enhance its privacy program in response to legislative requirements and breaches of FDIC employee information.

However, we identified opportunities for the FDIC to strengthen its privacy program for protecting personal employee information. These additional enhancements will help to ensure that 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.

[2] This Act is division H of the Consolidated Appropriations Act, 2005, Public Law No. 108-447.
[3] A system of records refers to a group of records under the control of an agency from which information is retrieved by the name of the individual or by some other identifying particular assigned to the individual.

FDIC'S PRIVACY PROGRAM

In 2005, the FDIC appointed a CPO with overall responsibility for the Corporation's privacy program and designated a Privacy Program Manager to support the CPO in developing and implementing corporate privacy requirements. The CPO is in the process of implementing a number of privacy-related initiatives, including privacy training programs, to ensure FDIC employees and contractors are aware of and follow privacy requirements, policies, and practices.

However, the FDIC could do more to: (1) notify corporate employees about Privacy Act requirements and responsibilities and the existence of, routine uses for, and safeguards over personal employee information and (2) ensure effective implementation of Privacy Act provisions. In this regard, the FDIC lacks an overarching privacy policy to coordinate the CPO and traditional Privacy Act functions, specify key roles and responsibilities, and define key Privacy Act and sensitive information terminology. Further, the FDIC's Privacy Act directive is outdated and does not include roles and responsibilities for system managers who maintain records covered by a SORN. The FDIC could improve the *Unofficial Personnel System* (UPS), a SORN that has not been updated or republished in the *Federal Register* since 1989. The system covers a number of FDIC employee records, including records pertaining to parking permits, personnel awards, dental insurance, savings plans, retirement benefits, life insurance documents, and employee locator information. The Corporation could also improve other selected SORNs by disclosing that SSNs are maintained in these systems of records. These improvements will help ensure that the FDIC fully complies with the Privacy Act provisions.

Chief Privacy Officer Brought Renewed Focus to Corporate Privacy Program

In March 2005, in response to Section 522, the Chairman appointed the Chief Information Officer (CIO) and Director, Division of Information Technology (DIT), as the CPO for the FDIC.[4] In the appointment letter, the Chairman designated the CPO "… with responsibility for those duties assigned to that position by law and by administrative action, and with overall agency-wide responsibility for information privacy issues." The Legal Division prepared a memorandum describing the roles and responsibilities of the designated privacy official and subsequently provided its analysis to the CPO, outlining CPO requirements and responsibilities. Appendix III presents information from the Legal Division memorandum describing CPO responsibilities, reporting requirements, and other specific tasks.

The CPO brought a renewed focus to the FDIC's privacy program and introduced a number of initiatives, including establishing a task force to evaluate FDIC procedures over sensitive information maintained electronically, designating a Privacy Program Manager to enhance the FDIC's privacy program, and addressing OMB's FISMA-related reporting guidance regarding privacy.

Risk Mitigation Project Team: In early 2005, the CIO established the Risk Mitigation Project Team (Team) to evaluate areas within the Corporation where new or improved procedures might be needed with respect to safeguarding sensitive information held by the FDIC in an electronic format. For the first phase of the project, the Team members chose to limit their review to electronic information that is stored, transmitted, or transported outside the FDIC. On

[4] The Director, DIT, was also designated as the FDIC's senior official for privacy for purposes of OMB's Memorandum M-05-08, *Designation of Senior Agency Official for Privacy*, dated February 11, 2005.

March 30, 2005, the Team submitted a memorandum to the CIO Council[5] that identified three general areas in which the Team thought immediate attention was necessary to develop:

- an FDIC-wide policy on what is to be done if sensitive personal information is lost or inappropriately disclosed,
- a single policy or a centralization of all FDIC policies on safeguarding sensitive information, and
- a corporate culture that embraces the importance of protecting sensitive information.

The Team prepared:

- a brochure covering protection of sensitive data, protection of mobile data storage devices (such as laptops and flash drives), the importance of rapidly reporting the loss or theft of these items, and a contact number; the brochure was later enhanced to cover protection of sensitive data in hardcopy as well as electronic format;
- a wallet-sized card containing the contact information for reporting the loss or theft of data or mobile storage devices; and
- a Web site providing online reference to protection of data and mobile storage devices and the way to report losses of data or devices.

In October 2005, the CPO sent a global message to all FDIC employees and contractors in regard to protecting sensitive information. The CPO's message announced: the impending release of the brochure and the wallet-sized card to employees and contractors; that the Privacy Web site had been posted; and that DIT was issuing luggage tags with FDIC contact information to employees and contractors with FDIC laptops in the event that the laptop was lost or stolen.

FDIC Privacy Program Manager Enhancements: The CPO designated a Privacy Program Manager in April 2005 to enhance and implement a comprehensive privacy program. The objective of the CPO's enhanced privacy program is to ensure that the FDIC is taking appropriate steps to protect personal information from unauthorized use, access, disclosure, or sharing and to protect associated information systems from unauthorized access, modification, disruption, or destruction. Table 1, on the following page, depicts the numerous initiatives of the privacy program and their status as of October 31, 2005.

The CPO also indicated that his office was performing a gap analysis between the Legal Division's list of CPO requirements, discussed earlier, and privacy program initiatives in place. The Privacy Program Manager kept us apprised of developments in the privacy program through periodic status reports on the work products supporting the Program, the staff assigned to various initiatives, and the estimated completion dates for the initiatives.

[5] The FDIC's CIO Council advises the CIO on all aspects of adoption and use of information technology at the FDIC.

Table 1: FDIC Privacy Program Initiatives

Area	Initiative	Estimated Completion	Status as of October 31, 2005
Governance	Create a senior-level Privacy Advisory Council to advise the CPO.	November 2005	Privacy Advisory Council directive was drafted, but a decision was made to incorporate these responsibilities into the mission of the CIO Council, whose members will vote on the change to the charter during a November 2005 meeting.
Policy	Develop an approach for reviewing and consolidating existing privacy directives and policies.	November 30, 2005	Circular 1031.1 has been updated and is currently being processed for approval within the Corporation. Circular will be retained. As part of the overarching privacy policy, prepared a list of directives, policies, and Web sites that contain privacy-related requirements. Plan to perform analysis of and determine how, collectively, the directives, policies, and Web sites protect sensitive personal data.
Privacy Web site	Establish a Web site providing a single source for privacy requirements, policy, education, reference, and documentation.	Completed	Privacy Program Web site www.fdic.gov/about/privacy available in early September.
Privacy Training	1. Privacy Briefing for senior managers. 2. Standalone online privacy training for all employees and contractors. 3. Approach for developing online privacy training as part of annual Security Awareness training for all FDIC employees. 4. Approach for developing in-depth online privacy education. 5. Classroom privacy training.	1. Completed 2. Completed 3. December 2005 4. December 2005 5. Currently not contemplated	1. CIO Council training completed on September 6, 2005. 2. October global e-mail sent to all employees and contractors regarding mandatory privacy training. 3. Security staff review indicated that the Department of Interior (DOI) training module might be a good substitute for current FDIC Security module, with minor strengthening of the Privacy portion. 4. Pending decision on DOI module, which could also be used for in-depth training. 5. A 96-slide PowerPoint presentation is available but needs Corporate University "branding".
Privacy Awareness	1. Prepare an e-mail to all employees and contractors regarding protection of sensitive information. 2. Send a package of material to employees and contractors, consisting of a brochure, wallet-sized card, and a luggage tag, addressing the need to protect sensitive data in electronic or paper format. 3. Update Incident Reporting and Response Procedures. 4. Prepare articles on the privacy program for the *FDICNews*.	1. Completed 2. Completed 3. November 2005 4. Ongoing	1. October global e-mail sent to all employees and contractors. 2. Distribution of brochure and wallet card to employees and contractors began on October 18, 2005. Luggage tags were issued to laptop users. 3. Current procedures have been updated and sent to the Privacy Program Working Group for concurrence prior to implementation. A meeting was scheduled for the week of November 14, 2005 to discuss final changes. 4. Article appeared in the *FDICNews* September 2005 issue. The next article is slated for the December 2005 issue.
Privacy Impact Assessments	A Privacy Impact Assessment will be prepared for each information system containing personal information.	Completed	All Privacy Impact Assessments have been completed and posted on the Privacy Program Web site.
Reporting	1. FISMA Section D *Privacy*. 2. OMB A-130 Reviews. 3. Initiate review of SORNs. 4. Memorandum to the Inspector General from the CPO.	1. Completed 2. Completed 3. December 2005 4. Completed	1 and 2. Final transmittal to OMB occurred on October 7, 2005. 3. In planning phase. Meeting was held with Privacy Act Clearance Officer. 4. Memorandum was sent to the Acting Inspector General on September 15, 2005.

Source: July 2005 Privacy Act Presentation to the FDIC Operating Committee and Privacy Program Status Reports.

FISMA Section D, *Privacy*, Questions: The OMB's June 13, 2005 memorandum (M-05-15) entitled, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, directs the senior agency official for privacy to answer a series of questions regarding the agency's privacy programs. The OMB memorandum also encourages agency Inspectors General to provide meaningful information on their respective agency's privacy program and activities. The CPO provided a memorandum to the OIG, as required, detailing the FDIC's privacy and data protection policies and procedures, summarizing the Corporation's use of information in an identifiable form, and verifying the CPO's intent to ensure that the Corporation's privacy program complies with federal statutes and federal and corporate policies and procedures.[6]

AREAS FOR IMPROVEMENT – PRIVACY PROGRAM

The FDIC has taken or initiated actions designed to strengthen and enhance its privacy program. However, the FDIC could do more to communicate Privacy Act requirements and responsibilities to its employees and to ensure effective implementation of Privacy Act provisions. In this regard, the FDIC needs to develop policy to coordinate CPO and Privacy Act requirements. The FDIC also needs to update the UPS SORN and revise other SORNs.

Overarching Privacy Policy Needed to Coordinate CPO and Traditional Privacy Act Responsibilities

Section 522, enacted on December 8, 2004, requires, within 12 months of the enactment, that each agency establish and implement comprehensive privacy and data protection procedures governing the agency's collection, use, sharing, disclosure, transfer, storage, and security of information in an identifiable form relating to agency employees and the public. Such procedures should be consistent with legal and regulatory guidance, including OMB regulations, the Privacy Act, and the E-Government Act.

Existing Privacy Act Directive: FDIC Circular 1031.1, *The Privacy Act of 1974: Employee Rights and Responsibilities*, dated March 29, 1989, offers guidance to employees about the rights provided and the responsibilities imposed by the Privacy Act. Circular 1031.1 was last revised in 1989. The Corporation is updating Circular 1031.1 and recently transmitted a draft directive to divisions and offices for review and comment. In its present and revised form, the circular includes general responsibilities for the Corporation and employees, definitions of the terms "record" and "system of records," and procedures for access to records.

However, neither this circular nor other FDIC directives provide a comprehensive description of the FDIC's privacy and data protection procedures. Elements that should be addressed include:

- the role, responsibilities, and coordination activities of the CPO, Privacy Program Manager, the Privacy Act Clearance Officer, and FOIA-PA Group;

[6] The OIG issued 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 2005. The report concluded that although the FDIC had taken a number of actions to protect information in an identifiable form, the FDIC needed to complete ongoing initiatives related to: (1) identifying all FDIC-maintained information in an identifiable form and taking appropriate actions to ensure this information is properly protected; (2) reviewing privacy policies and procedures to ensure they are current, comprehensive, and complete; and (3) implementing a corporate-wide training and education program, including job-specific training where appropriate.

- definitions for Privacy Act information and for other sensitive information terminology, such as "personally identifiable information" and "information in an identifiable form";
- references to key privacy-related federal laws, in addition to the Privacy Act, such as the E-Government Act of 2002, Paperwork Reduction Act, FISMA, and Section 522;
- OMB privacy-related requirements, such as OMB Circular No. A-130, Appendix I;
- roles and responsibilities of system managers; and
- procedures for creating, altering, or terminating a system of records.

Privacy Program Initiative on Policy: As of October 31, 2005, the FDIC's Privacy Program Working Group had completed its research of existing corporate directives and policies that apply to privacy and started work on analyzing the directives, policies, and Web sites that contain privacy-related requirements to determine how the various sources work together to protect the FDIC's sensitive personal data. By November 30, 2005, the Privacy Program Working Group planned to develop an approach for developing an overall policy on privacy following the review of legal requirements and existing privacy-related policies and procedures.

The FDIC's Privacy Program Working Group should accelerate its activities in this area, especially in light of the December 8, 2005 date by which Section 522 stipulates that agencies are expected to implement comprehensive privacy and data protection procedures and strategies. The Privacy Program Working Group should consider the essential elements identified above in developing the overarching privacy directive.

Definitions for Privacy Act and Other Forms of Sensitive Information: The FDIC could benefit from using more clearly defined terms for Privacy Act and other sensitive information; defining the relevant legal framework to be applied, depending on the type of information; and establishing corresponding processes and procedures for safeguarding various types of information. We researched FDIC directives, circulars, and guidance as well as privacy-related laws and regulations to identify a standard definition for personal employee information and sensitive information. We identified numerous definitions in the documents we reviewed, some of which were similar and others that differed from each other. Some notable examples include:

- FDIC Circular 1031.1: Cites the Privacy Act definition of a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history that contains his or her name, or the identifying number (such as an SSN), symbol, or other identifying particular assigned to the individual, such as a fingerprint or voice print or a photograph.
- FDIC Web Privacy Guide: Defines personal information (or "personally identifiable information") as any data that identifies an individual, such as, name, e-mail address, home address, other physical address, telephone number, SSN, birth date, place of birth, birth certificate number, and any other data that identifies an individual.
- OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002: Uses the term "Information in Identifiable Form" and defines the term as information in an information technology (IT) system or online collection (a) that directly identifies an individual (e.g., name, address, SSN, or other identifying number or code, telephone number, e-mail address, etc.) or (b) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification.

None of the guidance we reviewed contained a standard definition of personal employee information. A standard definition could help ensure that all FDIC divisions and offices

consistently safeguard similar types of personal employee information. Appendix IV highlights some of the definitions contained in the various documents.

The FDIC Needs to Update and Republish the UPS SORN and Revise Other SORNs

The Privacy Act describes a system of records as a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other particular identifier assigned to the individual. The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a notice published in the *Federal Register,* which includes, among other things, the type of data collected, the types of individuals about whom information is collected, the intended routine uses[7] of the data, and procedures that individuals can use to review the information. Such SORNs provide FDIC employees and the public with information about the type of personal information the FDIC maintains on individuals, where that information is maintained, and the technical and administrative controls for safeguarding the information. Moreover, the SORN process helps to identify for the FDIC the type of information that needs to be protected.

OMB's guidance to agencies on implementing the Privacy Act states that the public notice provision is a key element of one of the Privacy Act's basic objectives, namely, to foster agency accountability through a system of public scrutiny. OMB Circular A-130, Appendix I, requires that agencies conduct biennial reviews of each SORN to ensure that the notice accurately describes the system of records and to publish changes in the *Federal Register*.

The FDIC currently maintains 24 systems of records whose notices were published at various times in the *Federal Register*. We determined that 12 of the 24 systems of records contained personal employee information. Detailed information about the location, storage medium, and safeguards listed in each of the 12 system of records is included in Appendix V. The FDIC amended and republished all of its SORNs in 2001, except for the SORN for the UPS. The FDIC has neither updated nor republished the SORN for the UPS since August 31, 1989. The UPS notice makes outdated references to:

- FDIC divisions and offices that are no longer part of the organizational structure (e.g., the Division of Liquidation, the Division of Accounting and Corporate Services, and the FDIC Office of Personnel Management).
- Discontinued corporate programs, such as the Upward Mobility Program.
- Incorrect system managers (e.g., the Division of Accounting and Corporate Services is listed as the system manager for Parking Permit Records and Employee Locator Records. DOA is now the system manager for those records).

In addition, because the UPS SORN has not been updated since 1989, the SORN does not address electronic storage media except for computer discs. Further, the UPS SORN states that computer discs are accessed only by authorized personnel, but the SORN does not mention system safeguards, passwords, access controls, or encryption in the storage section of the SORN, which is intended to identify the media in which records are stored. Furthermore, the SORN does not indicate the purpose for the system of records, which subsequent to 1989, became a requirement by the Office of the Federal Register.

[7] According to the Privacy Act, the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose that is compatible with the purpose for which it was collected.

Over time, changes in agency operations or functions may result in increased differences in the records that are contained within a common system of records. Groups of records that once were appropriately combined into a common system may become sufficiently different so that they should be divided into separate systems. In this regard, the UPS SORN identifies seven categories of records broadly defined as personnel-related records that are maintained in addition to those kept in the Office of Personnel Management-required Official Personnel Folders (OPF). Our observations regarding the UPS SORN are in Table 2. Appendix VI lists and describes the seven categories of records in the UPS SORN.

Table 2: OIG Observations Regarding the UPS Notice

	Condition	Criteria	Effect
Updates to the UPS SORN	FDIC SORN 30-64-0015, UPS, has not been updated since 1989 and is listed in the FDIC Rules and Regulations (30-64-0001, *et seq.*) with a note stating "to be revised at a later date."	The Privacy Act requires that agencies maintain all records that are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual. OMB Circular No. A-130, Appendix I requires agencies to review SORNs biennially to ensure they accurately describe the system of records.	Increases the risk the FDIC will make an adverse determination about an individual on the basis of incorrect information.
Publication of the UPS SORN in the *Federal Register*	The FDIC has not republished the UPS SORN in the *Federal Register* or on FDIC's public Web site. The FDIC revised all of its SORNs in 2001. Since that time, the UPS SORN, published in the *Federal Register*, has consisted of a qualifier that the SORN will be revised at a later date.	The Privacy Act requires agencies to publish in the *Federal Register* a notice of the existence and character of the system of records, when the system is established or revised. In response to a 1998 Presidential Memorandum regarding compliance with the Privacy Act, OMB Circular M-99-05, Attachment B, required agencies to review their systems of records to ensure that *Federal Register* notices were up-to-date and to publish a notice for any system of records previously overlooked.	Without a republished, updated UPS SORN, the FDIC cannot ensure that its employees can exercise their rights to access, review, and amend the records in the SORN, as guaranteed by the Privacy Act.
Categories of Records Within the UPS SORN	The UPS SORN includes a number of sources of employee information that could be presented in separate SORNs. The SORN references the following seven categories of records: 1. Personal Information on individuals. 2. Parking Permit Records. 3. FDIC Personnel Awards. 4. Dental Insurance Records. 5. Employee Locator Records. 6. Upward Mobility Files. 7. FDIC Savings Plan Records.	OMB Circular M-99-05, Attachment B, also required agencies to ensure their systems of records were not inappropriately combined. OMB noted that groups of records that have different purposes, routine uses, or security requirements, or that are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid possible lapses in security.	Inappropriately combined groups of records into one system of records limits the FDIC's ability to ensure that routine uses appropriate for certain groups of records do not also apply to other groups of records simply because they have been placed together in a common system of records.

Source: OIG analysis.

Contractor Information: We observed that, although not specifically required to do so, the UPS SORN does not indicate that Privacy Act information is located at an FDIC contractor's facility or that personal employee information data is being maintained by FDIC contractors. For example, the UPS SORN discusses the following information but does not refer to contractors or vendors doing work for the FDIC in these specific areas:

- FDIC Savings Plan Information: The FDIC has agreements with a trustee for investment and recordkeeping of the FDIC Savings Plan funds and provides the trustee Savings Plan data, records, computer programs, software, reports, and other documents.
- Dental Benefits Information: The FDIC has a contract with a vendor to provide administrative services for the FDIC Dental Benefits Program, including claim payments.
- Life Insurance Benefit Program Information: The FDIC has a contract with a vendor to provide life insurance for employees, dependents, and retirees.

The UPS SORN does identify that disclosures of information may be made, where relevant, to (1) the dental insurance carrier in support of a claim for dental insurance benefits and (2) the Savings Plan vendor so that it can carry out its functions as investor of the FDIC Savings Plan funds. However, the UPS SORN states that the records are located in the FDIC Office of Personnel Management, division or office levels in the FDIC Washington office, regional offices, and field offices. Records containing personal employee information are also located and/or maintained at contractor locations. Legal Division officials agreed to look into the matter.

We also discussed this issue with an OMB privacy official. The official stated that the focus should be on where the employee can get access to the records at issue, where they can request amendment to those records, and who is performing the accounting requirement under the Privacy Act relative to disclosures to third parties. If the location for such access, amendment, and accounting is a contractor location, then the location-of-records section of the SORN should indicate where the records are located. Moreover, according to the official, if the contractor is performing Privacy Act-related responsibilities, the agency's contract with the contractor should specify those responsibilities. The OMB official noted that even if access, amendment, and accounting are handled through the agency, nothing precludes the agency from indicating in the SORN that the records are maintained by a contractor.

Observations on the FDIC's Other SORNs: We observed that SORNs did not always fully describe certain required information, such as all locations where the records are maintained or certain other categories of records maintained in the system. In addition, although not required to do so, several SORNs did not disclose that SSN information was contained in the system of records. For example:

- *Employee Training Information Records* (30-64-0007): The categories of records in the system do not identify the SSN as information contained in the records, but the SORN indicates that electronic media are accessible by SSN for retrieval purposes.
- *Financial Information Management Records* (30-64-0012): The categories of records in the system do not identify the SSN as information contained in the records, but the SORN indicates that electronic media are retrievable by SSN or specialized identifying number. In addition, the SORN does not reflect Public Transit Subsidy Program[8] payments in the categories of records in the system, despite the fact that the application for this program

[8] On January 13, 2000, the FDIC approved for corporate employees a Transit Subsidy Program designed to encourage employees to use mass public transportation, thereby reducing the use of private automobiles for daily commuting. DOA manages this program.

specifically identifies the Financial Information Management Records SORN in its Privacy Notice.

- *Employee Medical and Health Assessment Records* (30-64-0017): The SORN does not indicate that the records contain SSNs. In addition, the SORN does not disclose that records are located at the FDIC's 801 Building location. The routine uses stated in the SORN do not refer to disclosures to the Department of Health and Human Services with respect to the National Directory of New Hires.[9]
- *Fitness Center Records* (30-64-0021): The SORN does not indicate that the records contain SSNs. In addition, the SORN does not disclose that records are located at the FDIC's 801 Building location.

Recommendations

We recommend that the CPO and General Counsel:

1. Develop and issue an overarching privacy policy to include:

    - coordination and reporting responsibilities and expectations among the CPO, the Privacy Act Clearance Officer and FOIA-PA Group, and SORN system managers;
    - references to other relevant privacy and information security directives;
    - key roles and responsibilities, including SORN system manager responsibilities; and
    - definitions for information subject to the Privacy Act and for other sensitive information terminology, such as "personally identifiable information," and "information in an identifiable form."

2. Revise and republish the SORN for the *Unofficial Personnel System* to include updated, accurate:

    - information about records maintained;
    - references to FDIC offices, system managers, and safeguards over information; and
    - identification in the *System Location* section of information being maintained by contractors or vendors.

3. Determine whether records detailed in the SORN for the *Unofficial Personnel System* should be republished as separate, individual systems of records.

[9] According to the *Personal Responsibility and Work Opportunity Reconciliation Act of 1996*, as amended, federal agencies are to provide certain information about newly hired employees to the U.S. Department of Health and Human Services' National Directory for New Hires. In 1997, OMB issued suggested "routine uses" statements regarding disclosure to the Directory.

FDIC PRACTICES AND INITIATIVES TO PHYSICALLY SAFEGUARD PERSONAL INFORMATION

DOA and DOF implemented a number of controls for safeguarding personal employee information, including administrative and physical safeguards such as: limiting access to human resources operations and files; securing office space; eliminating SSNs from most forms and standard reports; and installing personal shredders and locked, high-volume shredding bins. Further, DOA and DOF had several additional initiatives underway to safeguard information.

However, we found that Human Resource Branch (HRB) contracts did not always contain Privacy Act references, confidentiality clauses, or signed confidentiality agreements. We also identified opportunities to increase physical safeguards over personal employee information such as strengthening controls in regional HRB offices, discontinuing the maintenance of unofficial personnel files, and developing limitations on information that student interns may access. We also noted that the FDIC included employees' SSNs in information on the FDIC's mentoring program provided to a contractor, rather than using an alternative identifier. These improvements will help to ensure that the FDIC implements sufficient physical controls over personal employee information.

***Sources of Personal Employee Information*:** We focused our review on DOA and DOF because the two divisions have responsibility for maintaining human resources, payroll, and supplemental payment information on FDIC employees. Table 3 presents the sections and branches within DOA and DOF that work with or maintain personal employee information.

Table 3: DOA and DOF Sources and Uses of Personal Employee Information

Section or Branch	Sources and Uses of Information
DOA	
Human Resources Service Center	Official Personnel Folders. Applications for FDIC employment.
Benefits Center	Benefits information (e.g., health, vision, and dental) for current FDIC employees and retirees. Benefit files for deceased employees.
Strategic HR Services and Labor/Employee Relations	Disciplinary and adverse action case files.
Human Resources Information Management and Payroll	Employee time and attendance and other payroll records; employee personnel action records; and staffing tables.
Corporate Recruitment and Career Management Services	Employee counseling information; employee résumés; mentoring program information; and training rosters.
Facilities Operations Section	Health Units--Employee medical folders. Fitness Centers--Employee membership and termination of membership; related payroll deduction forms; and medical history, clearance, and authorization forms.
Security Management Section	Personnel suitability (background) investigations on FDIC employees.
Corporate Support Section	Long-term, off-site records storage and shredding services.
Management Services Branch	Unofficial Personnel Files for DOA and Corporate University (CU).
DOF	
Accounting Operations Section	Account reconciliations for: employee receivables; payroll-National Finance Center (NFC) accounts; employee home purchases and selling; employee-deferred bonuses; and employee buyouts.
Receipts and Disbursements Operations Section	Supplemental payments—life cycle, petty cash. Travel voucher reviews, including Frequent Travel Lodging Stipend and Travel Card Program. Relocation payments and buyout payments.

Source: Interviews with DOA and DOF officials.

DOA and DOF business practices and initiatives for safeguarding personal employee information are discussed in the next section. For each process, we identified: the administrative, physical, and technical controls over personal employee information; the number and position of staff with access to the information; systems used to maintain and process the information; and whether contractors had access to the information. We also observed the physical location of hardcopy information stored in FDIC office space and verified that physical security controls were in place.

The FDIC Has Established Practices and Initiatives for Safeguarding Personal Employee Information

The Privacy Act requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure 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 on whom the information is maintained." In addition, with respect to privacy and security, the Paperwork Reduction Act of 1995 requires agencies to "implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for the agency" and "identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency." Both the Privacy Act and the Paperwork Reduction Act are applicable to the FDIC.

The FDIC has established or initiated numerous practices for safeguarding personal employee information in hardcopy form. DOA has taken the following actions to safeguard personal employee information:

- Human Resources (HR) personnel and security management offices that handle or process personal employee information are housed in limited access, secured office space. Cipher-lock doors have been installed to control access to work space.

- Official files that contain SSNs, such as OPFs, Labor/Employee Relations case files, and HR benefits files, are kept in locked file cabinets and/or rooms with limited and monitored access. Individuals conducting OPF file reviews, other than an HR specialist and Legal Division representative, must present identification and receive continuous oversight during the review.

- As of June 2004, DOA's Records Management Unit converted full SSNs to truncated SSNs on most FDIC forms.

- HRB has either discontinued producing most of its standard reports containing SSNs or restructured its reports to omit SSNs.

- HRB headquarters ordered personal shredders for each of its employees. Records Management installed secured shredding bins throughout FDIC Headquarters offices. Only the vendor and a member of Records Management have keys to the padlocked shredding bins.

DOF also has taken specific steps to safeguard employee sensitive information:

- DOF staff views employee SSNs only during the year-end Internal Revenue Service (IRS) Form W-2[10] reconciliation process. The W-2 forms are printed on a special DIT computer, DOA staff place the forms in envelopes, and the mailroom sends the forms to FDIC employees. DOF stores W-2 forms for 3 years on-site in locked file cabinets inside a cipher-locked file room, after which the W-2 forms are shipped to Iron Mountain (an FDIC off-site data storage vendor).

- Similar to DOA, in September 2004, DOF's Travel Audit Unit reissued its travel policies, established the use of a truncated SSN in lieu of the full SSN, and requested deletion of SSNs from standard travel forms. A written justification must be submitted to DOF management for review in order to use a full SSN on forms.

- Travel audit, relocation, and credit card files containing personal employee information are stored in locked file cabinets or cipher-locked file rooms with limited access.

- DOF is reviewing its relocation program processes and systems that contain personal employee information and is changing its hardcopy forms to only require truncated SSNs.

Further, the FDIC has taken steps to raise FDIC employee awareness about safeguarding sensitive data, including personal employee information:

- In November 2004, the Associate Director, HRB, sent a reminder to HR Washington, D.C., staff regarding the guidance for determining what is considered "sensitive information," including FDIC's Circular 1031.1 on the Privacy Act and United States Office of Personnel Management's (OPM) Operating Manual, *The Guide to Personnel Recordkeeping*.

- In August 2005, DOF reissued a memorandum on *Managing DOF's Confidential Records,* previously issued in June 1997 and August 2000. The memorandum reminded staff of the importance of safeguarding confidential and sensitive materials and protecting confidential information from unauthorized use or disclosure.

- DIT's Enterprise Architecture Board (EAB) initiated a corporate-wide survey to collect information about sources (electronic as well as hardcopy) of data within the Corporation that contain sensitive information and were outside of major information systems. Sources of data included in the survey were shared drives, personal drives, Access databases, and Excel spreadsheets.

- The FDIC's CPO is developing an awareness campaign, including the Privacy Program Web site;[11] privacy questions in the annual computer security awareness training; and separate privacy awareness training mandatory for all employees and contractors. The CPO issued a brochure in October 2005 to all employees regarding the safeguarding of sensitive information in electronic and hardcopy form.

[10] IRS form W-2 is an individual's wage and tax statement, which includes information such as name, address, and SSN.
[11] Privacy Program Web site established as of September 9, 2005.

AREAS FOR IMPROVEMENT – PHYSICAL SAFEGUARDS

Contracts Did Not Always Contain Privacy Act References, Confidentiality Clauses, or Signed Confidentiality Agreements

The Privacy Act provides that when an agency contracts for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency is responsible for causing the requirements of the Act to be applied to such a system. Subsection (m) of the Privacy Act further specifies that any such contractor and its employees are considered to be employees of an agency under the Privacy Act for purposes of the Act's criminal penalties. OMB Circular A-130, Appendix I, describes agency responsibilities for implementing Privacy Act reporting and publication requirements. The Circular requires agencies, every 2 years, to conduct a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to ensure that the wording of each contract makes the provisions of the Privacy Act binding on the contractor and his or her employees.

We identified a total of 15 DOA and DOF contracts and agreements for employee benefits, file room maintenance, and other services involving the maintenance of personal employee information. We reviewed the contract documents and contract files for references to the Privacy Act, confidentiality clauses, and evidence of signed contractor confidentiality agreements, as presented in Table 4.

Table 4: DOA and DOF Contracts Involving Personal Employee Information

Contractor or Vendor	Privacy Act Reference	Confidentiality Clause	Signed Confidentiality Agreement
Benefits Allocation Service (BAS)—Flexible Cafeteria Benefits Program	Yes	No	No
Vision Service Plan	No	No	No
Connecticut General Life Insurance Company (CIGNA)	No	No	No
Aon Consulting	No	No	No
MetLife	No	No	No
Labat Anderson	Yes	No	No
JHM Research & Development, Inc.	Yes	No	No
Contract Consultants	No	No	No
Ikon	No	No	Yes
Cendant	No	Yes	No
Scheduled Airlines Traffic Offices, Inc.	Yes	No	No
Impact Training Systems	No	No	No
Career Development Leadership Alliance	No	No	No

Source: OIG analysis of contracts and contract files.

As shown, we found that the FDIC did not consistently require that DOA and DOF contracts involving personal employee information include references to the Privacy Act or appropriate confidentially clauses, or that contractors sign confidentiality agreements. In addition, we identified two FDIC agreements with vendors that provide financial and payroll services, namely, T. Rowe Price and NFC. The T. Rowe Price trust agreement included a confidentiality clause, but not a Privacy Act reference, while the NFC interagency agreement included a Privacy Act reference, but not a confidentiality clause.

Privacy Act References: The FDIC *Acquisition Policy Manual* (APM) states that a contractor who designs, develops, or operates a system of records regarding personal information, in order to accomplish an FDIC function, must comply with the Privacy Act, and the Contracting Officer will ensure that the Privacy Act is included in all contracts, as appropriate. As shown in Table 4, the FDIC's contract with the BAS to administer the Flexible Cafeteria Benefits Program contained a one-page discussion requiring the contractor to comply with the Privacy Act and explaining civil and criminal penalties that could result from Privacy Act violations. However, we did not find Privacy Act references in other employee benefits contracts. A Legal Division representative indicated that the benefits contracts should have included references to the Privacy Act.

Under the Privacy Act, agencies are to require that systems of records operated on the agency's behalf under contracts be operated in conformance with the Act. Failure to do so may result in civil liability to individuals injured as a consequence. Moreover, a Legal Division representative noted that the Privacy Act is an operational law and that contractors are bound by the Privacy Act for *intentional* violations of the Act, regardless of whether the Act is specifically referenced in a contract. However, the Privacy Act does have limitations, and a contractor would not necessarily be bound by the Privacy Act in the event of *negligent* violations. The Legal Division representative concluded that it was important for FDIC contracts to reference the Privacy Act in order to hold contractors accountable in the event of violations resulting from carelessness or negligence.

The Legal Division representative indicated that Legal representatives would work with the Acquisition Services Branch (ASB) to develop a Privacy Act contract clause, similar to the clause in the BAS contract and require this clause to be standard language in all FDIC contracts, whether or not those contracts involve Privacy Act information. Further, the representative indicated that the Legal Division will work with ASB to issue modifications to contracts with the other contractors or vendors listed in Table 4 to include Privacy Act references.

Confidentiality Clauses and Confidentiality Agreements: The FDIC standard contract, used for most procurement actions, contains the following clause that requires a contractor to maintain, on a confidential and non-disclosure basis, any information that it acquires from the FDIC.

> Contractor must ensure the confidentiality of all information, data, and systems provided by FDIC or used or obtained by Contractor personnel under this contract and prevent its inappropriate or unauthorized use or disclosure. Contractor and all employees working on an FDIC contract must sign the Contractor Confidentiality Agreement (attached) no later than five (5) business days after starting performance and prior to receiving such information, or when receiving their badges, and return the signed Agreements to the Contracting Officer. This includes Contractor personnel who are required to work on-site at an FDIC facility or have access to FDIC sensitive information or data, systems or network. Failure to provide the signed Agreements may result in the removal of the employee from performing under the contract.

Further, the FDIC APM states that a contractor shall be required to sign a confidentiality agreement, prior to being provided the sensitive information, where a contract requires the rendering of goods or services that are of such a nature that the contractor will receive or might have access to information of a confidential nature, or where the contractor is required to work on-site at an FDIC facility, or has access to information of a sensitive nature.

As shown in Table 4, most of the contracts that we reviewed did not include the confidentiality clause. Further, we were unable to find signed contractor confidentiality agreements for most of the contracts that we reviewed. ASB officials could not definitively explain why the confidentiality clauses were not included in the signed contracts or why confidentiality agreements were not executed for these contracts but surmised that ASB staff mistakenly understood that the clause and confidentiality agreements were required only for DIT-related information technology contracts.

In Evaluation Report No. 00-006, *FDIC's Information Handling Practices for Sensitive Employee Data*, dated October 11, 2000, we reported that the FDIC did not have a confidentiality agreement in place for CIGNA, one of the contractors listed in Table 4. Because the FDIC indicated that it would work with CIGNA to establish a confidentiality agreement, we did not make a formal recommendation in the 2000 evaluation report. However, the current CIGNA contract still does not have a signed confidentiality agreement.

According to a Legal Division representative, confidentiality agreements provide an additional level of protection for the FDIC in the event of Privacy Act violations or inappropriate release of confidential information. However, the representative indicated that the FDIC would not be vulnerable in the event that confidentiality agreements were not signed. Nevertheless, the Legal Division representative indicated that confidentiality agreements are important and that confidentiality clauses and confidentiality agreements should be included in contracts involving access to personal employee information.

With respect to whether confidentiality agreements should be required for each contractor employee, a Legal Division representative stated that, ideally, the FDIC should have an officer of the contractor sign a single confidentiality agreement on behalf of the contractor and then certify that individual contractor employees have been apprised of Privacy Act requirements and the importance of maintaining the confidentiality of FDIC data.

Legal Review of Contract Before Contract Award: We concluded that the HRB contracts that we reviewed were not consistently subject to review by the Legal Division before contract award. Legal Division representatives indicated that their division is usually involved in reviewing the contract solicitation package.[12] However, the Legal Division is not always involved in reviewing the final version of the contract before the contract is signed, and ASB is not consistently providing the division with executed copies of contracts.

The FDIC APM identifies the Contracting Law Unit within the FDIC's Legal Division as a member of the team supporting the FDIC's contracting process. The unit supports the development of contracting policy and procedures and provides advice and legal sufficiency reviews. The APM stipulates procurement responsibilities for the Legal Division, including requirements to (1) review solicitation packages for contracts of $100,000 or more; (2) review complex contracting requirements, as requested by the Contracting Officer (CO); (3) provide advice as required on issues involving contract scope; and (4) provide other assistance as requested by the CO. The APM does not specifically require that the Legal Division review contract documents unless requested by the CO. In a prior evaluation, we reported the need to involve the Legal Division in procurement planning and in the review of key contracting

[12] The solicitation package includes the request for proposal, a draft copy of the proposed contract, and the proposed SOW.

documents such as the contract and SOW prior to contract execution,[13] and we still consider Legal Division involvement to be a valuable control.

In January 2005, ASB issued an interim policy memorandum establishing a process for coordinating legal reviews of contractual actions and supporting documents, which specified that the CO and Contract Specialist are responsible for obtaining the appropriate level of legal review and approval for solicitation and contracting actions. The contracts discussed in this report predated ASB's interim policy. Accordingly, we did not evaluate the effectiveness of the interim policy in ensuring adequate Legal Division review of key contractual documents.

Safeguards Over OPFs Were Less Stringent in Regional Offices, and DOA Continues to Maintain Unofficial Personnel Files

OPM issues government-wide guidance on documenting individuals' federal employment through its *Guide to Personnel Recordkeeping*, which, among other things, requires agencies to:

- implement management controls to ensure that personnel records are protected against loss or alteration;
- ensure that personnel records subject to the Privacy Act are secured against unauthorized access (for example, paper or microfiche/microfilmed personnel records subject to the Privacy Act should be stored in locked file cabinets or in secured rooms);
- limit access to personnel records subject to the Privacy Act to those employees whose official duties require such access (limitation applies to paper, microfiche/microfilm, and electronic records); and
- establish procedures to allow employees or their designated representatives access to their own records (procedures should ensure that the records remain subject to the agency's control at all times).

HR Service Center representatives indicated that the FDIC follows requirements within this guide.

We interviewed officials and observed file room operations for the Headquarters HR Service Center and HR centers in the Dallas and Atlanta regional offices. We identified one area wherein the three organizations were not fully complying with OPM guidance. Specifically, the three centers transfer OPFs to the National Personnel Records Center (NPRC) at varying times, as shown below, rather than following the OPM-recommended timeframes -- within 90 days of the employee's separation from federal service, or for a retirement or death, within 120 days, or until notification that a claim has been processed.

- **Headquarters HR Service Center** transfers OPFs within 2 months of an employee's resignation/termination, 6 months following a reduction in force, and 1 year after retirement or death.
- **Atlanta HR center** transfers an OPF within 1 year following an employee's termination, resignation, reduction in force, retirement, or death.
- **Dallas HR center** transfers an OPF within 6 months following an employee's termination, resignation, reduction in force, retirement, or death.

[13] Evaluation Report No. 04-014, *XBAT Contracting and Project Management*, dated March 26, 2004.

Timely transfers of OPFs to NPRC could help mitigate the risk of access to personal employee information. We also observed that the contract SOWs for the HR centers in Dallas and Atlanta do not specifically identify OPF file room tasks that should be performed. Further, contractor employees in the headquarters HR Service Center and Dallas HR center were not required to sign confidentiality agreements. We concluded that the headquarters HR Service Center, and Atlanta and Dallas HR centers, employ varying levels of controls over OPFs as illustrated in Table 5.

Table 5: OPF File Room Practices and OIG Observations

	Contractor-Operated OPF File Rooms	Confidentiality Agreements	Tracking OPFs	Transmission of Standard Form 75* (SF-75)
Criteria	As required in the FDIC's APM, the SOW should define the work products that are required and address all the elements necessary for successful performance by the contractor.	The FDIC APM requires a confidentiality agreement when a contract requires the rendering of goods or services that are of such a nature that the contractor will receive or might have access to information of a confidential nature, or where the contractor is required to work on-site at an FDIC facility.	The Washington, D.C., contract includes the requirement to log in and log out OPFs utilizing a barcoding system.	The Washington, D.C., contract includes the requirement to provide information using SF-75 to other federal and non-federal employers regarding FDIC employees. DOA Washington, D.C., HRB officials told us that DOA expects contractors to transmit SF-75s via certified mail and a confirmation receipt and identified this practice as a safeguard.
HQ HR Service Center	SOW identifies OPF File Room tasks performed.	No signed confidentiality agreement.	Uses Automated Records Management System (ARMS) through manual keying of SSN in lieu of the barcoding system. Also maintains a manual log book.	Contractor completes SF-75 and faxes to other agency. Does not request confirmation of receipt.
Atlanta HR Center	SOW does not identify OPF File Room tasks to be performed.	Confidentiality agreement signed by contractor employee.	Does not use ARMS. Uses manual log book and requires that OPFs be returned to the file room at close of business. Legal staff requires a management request and approval to remove an OPF.	HR completes form. Contractor mails form to other agency and signature of recipient is required.
Dallas HR Center	Contract is a GSA contract for temporary personnel services. SOW identifies the job classification of services contracted – does not identify OPF File Room tasks to be performed.	No signed confidentiality agreement.	Does not use ARMS. Uses an index card placed in a pocket of the temporary OPF file.	Contractor is not responsible for any tasks relating to the SF-75.
OIG Observations	SOW level of detail varies among the three contracts.	Only one contractor employee signed a confidentiality agreement.	No consistent practice of checking in/out OPFs. Washington, D.C., contractors do not follow the SOW requirement of utilizing the barcoding system for checking in/out OPFs.	Washington, D.C., contractor employees do not follow the practice of transmitting the SF-75 via certified mail or requesting a confirmation receipt.

Source: Interviews with HR service center staff in headquarters and HR center staff in Atlanta and Dallas and OIG observations and analyses.

* OPM Standard Form 75, *Request for Preliminary Employment Data*, is used by prospective employers to obtain pre-employment information about an applicant when the applicant's OPF is not available for review.

There are opportunities for DOA to strengthen its safeguards for protecting personal employee information stored in the OPFs. Without strengthening the controls and employing similar controls over official personnel folders in all HR centers, the FDIC could be more susceptible to Privacy Act violations or not fully complying with OPM guidance.

***Unofficial Personnel Files for DOA and CU Employees*:** Some FDIC divisions also maintain "unofficial personnel files" (UPF) or "working files." These files may contain various types of records with personal employee information including, but not limited to, SSNs, performance appraisals, and written notes and memoranda on employee performance. UPFs are included in the FDIC's UPS SORN, which states that the routine use for files in this system are for the employees' supervisors' use in preparing general personnel actions.

We met with the Administrative Officers (AO) in DOA, DIT, and Division of Supervision and Consumer Protection (DSC) to discuss their practices for safeguarding unofficial personnel files. DOA maintains unofficial personnel files containing training and personnel information on all DOA as well as CU employees. These files contain copies of the employees' SF-50s[14] which have SSNs, and the files are housed in locked filing cabinets in a locked file room. DOA told us that there are few requests to review the working files, and it is unusual to send a working file to a field office. Usually, employees and managers review the working files in lieu of the OPFs because of convenience. Although there is limited access to these working files, student interns may have access because they handle filing personnel information. DIT also told us that unofficial personnel files are maintained on all DIT employees. The files are stored in locked filing cabinets in a locked file room with access limited to the AO's staff.

We learned that DSC no longer maintains UPFs for its employees. In 2002, DSC returned these files to respective DSC employees. DSC told us that it did not see a need for these files once DOA decentralized and maintained OPFs in the regional offices. Also, with the exception of the New York Regional Office, each DSC regional office has an AO with access to personal employee information in the FDIC's Corporate Human Resources Information System (CHRIS) and New Financial Environment (NFE) for the AO's respective organization. Additionally, DOF does not maintain UPFs for its employees.

The Privacy Act states that agencies' systems of records should maintain only information that is relevant and necessary to a function that the agency is required to perform. OMB guidance states "in simplest terms, information not collected about an individual cannot be misused and agencies are to assess the relevance and need for personal information … whenever any change is proposed in an existing system of records." DIT and DOA may find it beneficial to assess the need for maintaining UPFs on DIT, DOA, and CU employees and should consider adopting DSC's and DOF's practices of not maintaining UPFs. Doing so would reduce the amount of personal information that requires protection.

Student Interns Continue to Have Access to Personal Employee Information

The FDIC's Student Educational Employment Program consists of two components: (1) the Student Temporary Employment Program which enables students to earn a salary and meet financial obligations while continuing their education, and (2) the Student Career Experience Program which provides students the opportunity to obtain work experience that is directly

[14] OPM SF-50 (*Notification of Personnel Action*) constitutes the official notice of a personnel action, including promotions, awards, bonuses, pay adjustments, and retirement plan information. The SF-50 contains personal employee information, including the employee's full SSN.

related to their education and career goals with the possibility of converting to a competitive appointment at the completion of the program. The FDIC's student interns (except for student interns employed by the OIG and the Chairman's Office) are designated as low-risk positions, and are defined as positions involving duties and responsibilities of limited relation to the FDIC or a corporate program mission. Low-risk positions are subject to a minimum background check.[15] OIG student intern positions are high risk and subject to a full background investigation.

As of May 2005, eight interns were working in HRB -- three student interns, four summer (student) interns, and one student trainee. Some of the student interns working in HRB had and continue to have access to personal employee information contained within the FDIC's human resources and payroll systems, computer files included in shared drives, and other sensitive hardcopy documents. For example, student interns in HR are responsible for boxing and shipping OPFs and merit promotion files, both containing personal employee information, including SSNs. One of the interns working in HR has open access to SSN information within CHRIS and NFC and responsibilities that include shredding HR documents and copying and delivering documents containing personal employee information.

Without limitations on student interns' access to personal employee information, the FDIC is at a greater risk that such information could be inappropriately accessed and misused. However, we acknowledge that some interns' duties and responsibilities might require handling personal employee information. In those cases, the FDIC needs to (1) ensure that the student interns participate in the Corporation's privacy awareness training courses or (2) expand the scope of the intern's background check. In addition, the FDIC should include discussions on safeguarding personal employee information in its student intern orientation seminars.

Mentoring Contractor Is Being Provided SSNs Without a Business Need

The FDIC adopted the Corporate Mentoring Program as a permanent corporate-wide program in 1999 to support a productive workplace by enhancing employees' job skills, empowering employees, and promoting good corporate citizenship. The FDIC Mentoring Program seeks to accomplish these objectives by helping less experienced employees (mentorees) draw upon the experience and knowledge of more experienced employees (mentors). The FDIC Mentoring Program is open to all employees[16] with participation typically limited to a maximum of 200 employees (100 mentorees and 100 mentors) for participation in a 1-year program. DOA Career Management Services administers the program.

During the annual open enrollment period for the FDIC Mentoring Program, applicants use an on-line application process to provide personal information such as name and SSN. The application includes the following Privacy Act statement regarding the collection of information:

> The information on this form may be disclosed in accordance with the other "routine uses of records" listed in the FDIC's Unofficial Personnel System, 30-64-0015. Your Social Security number (SSN) is requested to ensure record accuracy. Completion of this form is voluntary, but failure to provide the requested information, including your SSN, may result in your registration form not being processed.

[15] Low-risk positions are subject to a National Agency Check (which includes fingerprinting), a credit check, and inquiries to prior employers, educational institutions, and law enforcement agencies.
[16] Employees must have at least 1 year's experience with FDIC to participate in the Mentoring Program.

DIT developed and maintains DOA's database storing the information collected for the FDIC Mentoring Program, including applicants' SSNs. The database is released to an FDIC contractor that uses the information to develop biographical profiles on the applicants. This contractor has been providing the profiling services to the FDIC since 1999. The contract does not include a Privacy Act reference, confidentiality clause, or a confidentiality agreement.

According to DOA officials, in early October 2005, DOA discontinued the practice of including SSNs in the information released to the contractor. Specifically, DIT eliminated the SSNs from the mentoring database transmitted to the contractor and replaced the SSNs with different identification numbers.

DOA Career Management Services officials told us that they will consider using a different identifier other than the SSN for the 2007 mentoring program. Until DOA discontinues requiring the SSN in the mentoring program application, DOA risks maintaining employees' SSNs without a clear business need.

Recommendations

We recommend the Director, DOA, in conjunction with the General Counsel, Legal Division:

4. Prepare a standard Privacy Act contract clause for use in all contracts involving Privacy Act information.

5. Modify existing contracts discussed in this report to include specific references to the Privacy Act.

6. Require contracts that involve the electronic transmission of Privacy Act information to include encryption requirements.

We recommend that the Director, DOA:

7. Require HRB and DOF contractors listed in this report to sign contractor confidentiality agreements.

8. Remind contract specialists that they should not amend contracts or waive contractor confidentiality statement requirements without Legal Division concurrence.

9. Ensure that regional offices employ controls over official personnel files and any other personal employee information that are equivalent to those implemented by DOA's headquarters Human Resources Branch.

10. Evaluate and determine whether DOA should adopt DSC's practice of not maintaining Unofficial Personnel Files or "working files" and consider establishing a corporate-wide policy consistent with that practice.

11. Develop corporate guidelines detailing appropriate job tasks that interns should perform, and strengthen controls over interns' access to sensitive information.

12. Determine whether an employee identification number or other identifier could be used in place of employees' SSNs in the Career Management Services' mentoring program database.

FDIC PRACTICES AND INITIATIVES FOR SAFEGUARDING ELECTRONIC PERSONAL INFORMATION

The FDIC is actively reviewing information within its corporate systems and applications to determine which applications contain SSNs and employee identification numbers (EIN), collectively referred to as tax identification numbers (TIN), and is developing plans to remediate specific applications. The FDIC has also incorporated privacy questions into its processes for assessing the data sensitivity of applications and certifying and authorizing applications for operational use. The FDIC completed a Privacy Impact Assessment[17] (PIA) of 27 applications that the Corporation has identified as containing TINs and posted the PIAs to the FDIC's external Web site. We confirmed that CHRIS and NFE generally use a system-generated EIN, as opposed to an SSN, except in very few cases. We also verified that the FDIC limits employee access to SSN data within these systems.

However, we noted that the FDIC's PIA template does not address what opportunities individuals had to decline to provide information or consent to particular uses of information, an OMB requirement for agency PIAs. Further, opportunities may exist to impose document-level controls over electronic files containing Privacy Act information. Finally, contractors and vendors who maintain Privacy Act information for the FDIC, but are not connected to the FDIC's network, are not subject to any form of information security review or encryption requirement. These additional enhancements will help to ensure that the FDIC implements sufficient technical controls over personal employee information.

The FDIC Has Taken Proactive Steps to Identify Systems Containing SSNs

The OMB 2005 FISMA reporting instructions include a question related to the number of information systems containing federally owned information in an identifiable form and whether the agency has conducted a PIA and published SORNs. The FDIC is in the process of conducting a two-phased effort to identify SSNs in FDIC applications and in electronic files and hardcopy form.

Corporate Data Sharing Initiative: The FDIC began the Corporate Data Sharing initiative in 1997 to improve the sharing of corporate data assets within the FDIC and between the FDIC and financial institutions, the public, and other government agencies. The FDIC Corporate Data Sharing Steering Committee (CDSSC) is composed of representatives from all divisions and offices and sets the strategic direction for corporate data and information planning, management, and use. The FDIC has organized its corporate data into groups of related data, referred to as families, such as open institution data, procurement data, and FDIC personnel data. The CDSSC established Collaborative Working Groups (CWG) to manage each data family, develop descriptions of the data within each family, and establish business rules for the confidentiality, integrity, and availability of data within each family.[18] We reviewed the CDSSC business rules for the Corporate Personnel Data family, defined as information about FDIC employees, former employees, and candidate employees and found that CDSSC established business rules for the confidentiality, integrity, and availability of corporate personnel data.

[17] A PIA is an analysis of how information is handled (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

[18] Circular 1301.3, *Data Stewardship Program*, dated September 4, 2001.

Phase I of the SSN Project: In 2005, the CDSSC tasked the CWGs with assessing the FDIC's use of TINs. In Phase I of the effort, a small team searched all FDIC databases in the Enterprise Data Architecture for data elements that could indicate tax identifier data. The team then associated each data element to dependent application(s) and developed an inventory of applications containing TINs. In coordination with the DIT project manager, the team identified 62 of the FDIC's 313 applications as candidates that could reference TINs. After further analysis, the team ultimately recommended 26 applications for remediation to secure TINs within FDIC application systems and corporate databases.[19]

DIT's Data Management Section submitted a draft report entitled, *Corporate Use of Taxpayer Identification Number Remediation Analysis*, dated June 30, 2005, to the CIO. The draft report identified the 25 applications (later increased to 26), potential remediation methods, and cost estimates for remediating the applications. According to DIT representatives, the CIO considered the analysis to be a good first effort but concluded that the scope of the effort needed to be expanded. For example, the Phase I effort did not include NFE or legacy systems integrated with NFE. Further, remediation costs included the initial cost of reprogramming applications but may not have included the associated costs of testing the remediated applications or changes to business processes resulting from remediation.

Application Remediation Effort: DIT's Delivery Management Branch (DMB) group will be responsible for remediating specific applications. A DMB representative indicated that DIT would begin the remediation effort in early September 2005 after DIT had completed its reorganization. The representative stated that DMB had not established a time table or milestones for project completion and had not made cost estimates for the remediation effort. The representative also stated that DMB will likely prioritize the list of 26 applications to remediate those applications that present the most risk for the Corporation.

Phase II of the SSN Project: In August 2005, the CIO issued a memorandum to division and office directors, announcing the second phase of the SSN effort to collect information about electronic and hardcopy sources within the Corporation. This effort covered those systems that contain sensitive information in, for example, MicroSoft Word documents and Excel spreadsheets developed by individual employees or organizational units. The EAB gathered the information through an Internet survey. The CIO requested survey completion by September 23, 2005. According to DIT's October 2005 *Monthly Status Report to the Chief Operating Officer*, all divisions and offices reported their inventory items. The results will be analyzed and provided to the CPO.

The FDIC Completed Privacy Impact Assessments for Systems Identified as Containing SSNs

The E-Government Act of 2002 provides protection for personal information in government information systems or information collections by requiring that agencies conduct PIAs. The FDIC developed a PIA guide and template in July 2005. According to the *Privacy Program Status Report*, dated October 31, 2005, DIT had completed PIAs for 27 applications that it identified as containing SSNs. We reviewed the PIA template and the completed PIAs for five applications containing personal employee information. We compared the PIA to guidance contained in the E-Government Act and in OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated

[19] Remediation could include eliminating data fields within an application that contain SSNs or masking data fields containing SSNs so that system users are unable to view the SSN.

September 26, 2003. With the exception of one item, we concluded that the PIAs addressed each of the OMB-required elements as shown in Table 6.

Table 6: OIG Review of Selected PIAs

Did the PIA …	CHRIS	NFE	Training Server	Electronic Travel Voucher Processing System (ETVPS)	Multi-Tier Applications Architecture Project
Q1. Analyze and describe what information was to be collected?	Yes	Yes	Yes	Yes	Yes
Q2. Analyze and describe why the information was being collected?	Yes	Yes	Yes	Yes	Yes
Q3. Analyze and describe the intended use of the information?	Yes	Yes	Yes	Yes	Yes
Q4. Analyze and describe with whom the collected information was to be shared?	Yes	Yes	Yes	Yes	Yes
Q5. Analyze and describe what opportunities individuals had to decline to provide information or to consent to particular uses of information and how individuals could grant consent?	Not in PIA, but CHRIS Time & Attendance (T&A) login includes notice.	Not in PIA, but NFE login includes notice.	Not in PIA, Training Server does not include notice.	Not in PIA, but ETVPS login includes notice.	Not in PIA, but most FDIC employees do not access this system.
Q6. Analyze and describe how the information was to be secured (administrative and technological controls)?	Yes	Yes	Yes	Yes	Yes
Q7. Analyze and describe whether a system of records is being created under the Privacy Act?	Yes	Yes	Yes	No	Yes
Q8. Identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA?	Yes	Yes	Yes	Yes	Yes

Source: OMB Memorandum M-03-22 and OIG analysis of selected PIAs.

As shown, the PIAs that we reviewed did not address question 5. However, systems for three of the five PIAs that we reviewed contained the required notice at the system log-in screen. A DIT representative agreed to update the PIA template and the completed PIAs to address question 5.

We observed that DIT completed PIAs for all of its systems identified as containing TINs. OMB M-03-22 indicates that a PIA is not required where information relates to internal government operations, such as Web sites, IT systems, or collections of information that do not collect or maintain information in identifiable form about members of the general public. However, OMB encourages agencies to conduct PIAs on systems that collect information in identifiable form

about government personnel. A number of the applications for which the FDIC has conducted PIAs are internal systems that contain information about FDIC employees, but do not contain information about the general public.

FDIC Human Resources and Accounting Systems Limit the Use of SSNs

CHRIS, an integrated system that supports all existing FDIC HR functions, is based on the Federalized Commercial off-the-Shelf (COTS) HR software solution provided by PeopleSoft. CHRIS was implemented corporate-wide through four major releases spanning from February 2001 to May 2005, with the latest release, CHRIS T&A, being focused on time and attendance functionality.

CHRIS T&A System: The predecessor system to CHRIS T&A, the Corporate Time and Attendance Worksheet (CTAW), used employee names and SSNs to ensure record accuracy and for identification purposes. In a previous evaluation report issued in October 2000,[20] we reported that FDIC officials consistently identified CTAW as the area in which employee data was vulnerable, in part, because officials had observed in many instances that CTAW forms, containing SSNs, were left unattended in either in-boxes or on the desks of employees, supervisors, or timekeepers. As a result, officials believed that these forms could be seen by others who should not have access to this information. At the time of the prior evaluation, FDIC officials were in the process of replacing CTAW with CHRIS T&A and had planned to use a different EIN when CHRIS was implemented.

CHRIS T&A replaced CTAW as the FDIC's T&A system in May 2005. CHRIS T&A is a Web-based, employee self-service system that automates the leave and premium pay request process, provides an interface with NFE for accounting and cost management data, and is based on a COTS T&A system designed specifically for agencies using NFC payroll processing. The FDIC no longer uses SSNs for its T&A processing and has established unique employee identifiers – EINs– to replace SSNs. We reviewed CHRIS and NFC staffing tables and verified that the tables did not include SSNs.

CHRIS HR System: CHRIS HR is a human resources software solution developed in PeopleSoft and provides DOA with an integrated system to support existing HR functions. CHRIS HR provides employee information to NFE. Although CHRIS HR has SSNs, the FDIC has limited the number of individuals having access to the SSN field in CHRIS HR. We reviewed the CHRIS HR *Security Administrator User's Guide* and noted that it specified a number of security requirements for gaining access to the system.

In 2004, DOA conducted a security review to determine DOA employee access to sensitive computer systems and data, including CHRIS, and to ensure that the position risk level designations for employees having access to this information were proper in relation to the access. As a result of this security review, 208 DOA employees with CHRIS access had their position designations upgraded from low risk to moderate risk. Moderate-risk positions undergo a more extensive background investigation than low-risk positions.

NFE System: In May 2005, the FDIC implemented the NFE, an enterprise-wide, integrated software solution to support the financial needs of the FDIC. NFE modernized the FDIC's financial systems by implementing PeopleSoft functional modules to support existing business

[20] Evaluation Report No. 00-006, *FDIC's Information Handling Practices for Sensitive Employee Data*, dated October 11, 2000.

processes, absorbing legacy systems, renovating legacy systems not absorbed by NFE, and coordinating with CHRIS T&A developmental efforts that interoperate with NFE. NFE accesses SSNs only through the Payroll Module, which is a part of CHRIS HR, and the SSN is captured when the record is established for a new employee. The EIN is used at all other times. The NFE initiative established the following processes for electronically safeguarding personal employee information:

- NFE interfaces with the ETVPS, Relocation Management System, and Separation Incentive Payment System and automatically converts the SSN to the EIN when printing transaction reports or processing payroll. Two separate user identifications are required to view SSNs in CHRIS HR and NFE. Requests for system access are also subject to supervisory approval. DOF limits access to SSN data and reviews the NFE access levels every 6 months.

- All supplemental payments such as life cycle, petty cash, telephone reimbursements, and examiner/executive payments are coded by EIN and paid through the Payroll Module in lieu of the Accounts Payable Module. With the exception of the W-2s, all supplemental payments are printed out with the EIN instead of the SSN.

- The Payroll Bridge System interfaces with NFE and translates payroll data to create journal entries for the general ledger. The Payroll Bridge System creates files with SSNs and sends information to the Data Warehouse. However, to access data, DOF requires an employee to have two access roles and identification codes.

- ETVPS contains SSNs in electronic form. Truncated SSNs can be seen by a user, but the SSN cannot be printed from ETVPS. DOF has limited the access to the SSNs to nine employees in the Travel Audit Group and Security. DOF performs a semiannual reliability review of the data and a review of the user access levels to the ETVPS data. An employee is required to have an FDIC identification badge to access ETVPS, which contains the employee's Entrust[21] security profile.

In addition to the security efforts for NFE, DOF also initiated a project in July 2005 related to access control and maintenance of DOF's shared drive. This project consisted of a review of folders and associated sub-folders in the shared drive by the cognizant DOF manager to ensure that access to the folders and sub-folders is appropriate and that the need for the folder and its sub-folders still exists. DOF anticipated completing this project by the end of 2005 and established a goal to perform this type of review annually.

AREAS FOR IMPROVEMENT – ELECTRONIC SAFEGUARDS

Opportunities May Exist to Strengthen Document-Level Controls Over Electronic Documents Containing Privacy Act or Sensitive Information

Typically, organizations secure digital information by using perimeter-based security methods, such as firewalls, that limit access to a network, and access control lists, that restrict user access to specific data. Organizations may also use encryption and authentication technologies and products to help secure e-mail transmissions. Although these methods help to control access to sensitive data, they do not prevent recipients of such data from copying, printing, or

[21] Entrust is the software that the FDIC uses to encrypt and digitally sign e-mail messages and files.

further distributing sensitive information. For example, within the FDIC's network, a recipient of an encrypted file may forward the file, unencrypted, to another recipient.

Rights Management Services (RMS) is a relatively new technology from Microsoft for use with Microsoft Office 2003 and Windows Server 2003, which augments an organization's information security by providing protection of information through persistent usage policies that remain with the information, regardless of where it is sent. For example, persistent use technologies may:

- Prevent a recipient from copying, printing, saving, editing, or forwarding information to another recipient.
- Place time limits after which a document cannot be opened.
- Specify different rights for individual users (e.g., account managers are granted rights to alter or print data, while other users are limited to "read only" access).

The FDIC has instituted a number of effective controls at the system and application level. However, controls could be strengthened at the document level. RMS technology could provide a solution to enhance document-specific controls. During an earlier OIG audit of the FDIC's e-mail security,[22] we found that the FDIC had limited assurance that employees and contractors encrypt sensitive e-mail communications when required. We determined that technical shortcomings with the FDIC's implementation of encryption were a contributing factor for employees not encrypting sensitive e-mail communications. As a result, we recommended that DIT evaluate alternative solutions to augment its implementation of encryption for securing sensitive e-mail communications, including giving consideration to implementing RMS technology. In its response, DIT indicated that it was evaluating alternative solutions, including RMS, and would have the evaluation completed by November 30, 2005.

A key factor that DIT should consider in its evaluation is the Corporation's migration to Microsoft Office 2003 subsequent to our e-mail security audit. With this migration, the Corporation is in a better position to implement RMS. We intend to follow up on this issue by reviewing DIT's evaluation that was prompted by our prior recommendation.

The FDIC Needs to Require Some Form of Third-Party Security Review for Contractors and Vendors That Maintain Personal Employee Information in Electronic Form

The OMB 2005 FISMA reporting instructions[23] include guidance for federal agencies on the applicability of FISMA to government contractors. The OMB guidance references Section 3544(b) of FISMA,[24] which requires each agency to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The OMB guidance indicates that agencies must develop policies for information security oversight of contractors and other users with privileged access to federal data.

OMB also notes that FISMA requires agencies to provide security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of

[22] Report No. 05-016, *Security Controls Over the FDIC's Electronic Mail (E-Mail) Infrastructur*e, dated March 2005.
[23] OMB Memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated June 13, 2005.
[24] The reference to Section 3455(b) is a reference to 44 United States Code § 3455, which FISMA added to the Code.

the agency and for information systems used or operated by an agency or other organization on behalf of an agency. OMB further notes that agencies are fully responsible and accountable for ensuring that all FISMA and related policy requirements are implemented and reviewed and are included in the terms of a contract. OMB specifies that agencies must ensure identical, not "equivalent," security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation must, at a minimum, explicitly meet guidance from the National Institute of Standards and Technology. Agencies are also responsible for ensuring that contractor personnel receive appropriate training.

FDIC Contractor Security Guidance: FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*, dated June 30, 2003, establishes a framework for incorporating security into all phases of the IT acquisition process and for establishing IT security requirements for third-party providers who wish to provide automated data processing contract services or products to the FDIC. The scope of the circular applies to contractors and others who participate in IT contracting with the FDIC and to non-FDIC products and individuals that service, handle, manage, or interface with FDIC data or systems.

Among other things, the circular requires that connections to all FDIC platforms, operating environments, and applications be protected to prevent unauthorized access and assure accountability and integrity. Additionally, the circular requires security controls for the protection of sensitive data to be documented and provided to the contract oversight manager. The circular defines an automated information system as an application of information technology that is used to process, store, or transmit information.

DIT Contractor Security Reviews: Circular 1360.17 requires DIT Information Security Staff (ISS) to conduct periodic reviews of third-party servicers and COTS products for compliance with FDIC security policies and standards before, during, and following the period of contract performance or product service to the FDIC.

ISS has not performed security reviews of any of the HRB or DOF vendors discussed in Table 4 of this report. ISS indicated that Circular 1360.17 is intended for contractors who have direct connections to the FDIC's computer network. None of the contractors shown in Table 4 has direct connections to FDIC's computer network. ISS also questioned the feasibility of requiring contractors to maintain identical security controls or conducting security reviews at contractors that service multiple federal agencies. ISS noted that contractors with multiple federal clients could be subject to varying degrees of security controls and multiple security reviews by individual agencies. ISS indicated that the federal CIO Council had discussed the reasonableness of OMB's guidance and its repercussions at federal agencies and raised these concerns with OMB.

We agree that requiring identical security controls and conducting security reviews of contractors that do not have direct connections to the FDIC's network could be problematic, especially for contractors that work with multiple federal agencies. However, these contractors do maintain FDIC personally identifiable information, and the FDIC should be taking reasonable steps to ensure that contractors have adequate security controls in place commensurate with the risks and magnitude of harm resulting from unauthorized access to the information. We concluded there may be means to obtain assurances of adequate security for contractor-maintained information other than an ISS-performed security review as discussed below.

Third-Party Security Reviews: The increased use of technology and third-party service providers has resulted in complex systems and new business processes that increase productivity and efficiency but also increase the risks related to information security and privacy. Several entities have developed third-party programs to provide independent assurance about the security, availability, processing integrity, on-line privacy, and confidentiality of a contractor or service provider's Web site or computer system. Examples of third-party programs include the Council of Better Business Bureaus' award seals for on-line privacy and on-line reliability, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) Trust Services engagements, and the TruSecure Enterprise Certification.

AICPA/CICA Trust Services are professional assurance and advisory services based on core principles and criteria, presented in Table 7, that are designed to address the risks and opportunities of information technology. SysTrust and WebTrust are two specific services developed by the AICPA/CICA that are based on the Trust Services Principles and Criteria. SysTrust engagements provide assurance on the reliability of a computer system, while WebTrust engagements provide assurance on an organization's E-commerce system.

Table 7: AICPA/CICA Trust Services Principles and Criteria

Security	The system is protected against unauthorized access, both physical and logical.
Availability	The system is available for operation and use as committed or agreed to.
Processing Integrity	System processing is complete, accurate, timely, and authorized.
Online Privacy	Personal information obtained as a result of E-commerce is collected, used, disclosed, and retained as committed or agreed to.
Confidentiality	Information designated as confidential is protected as committed or agreed to.

Source: AICPA Web site.

Entities meeting Trust Services criteria are eligible to display the SysTrust or WebTrust seal on their system or Web site to indicate independent verification that an entity's system meets the Trust Services criteria. A Trust Services seal reveals the date the seal was granted and the date it expires, the site's business practices and policies, Trust Services Principles and Criteria used to examine the site, the report of the independent accountant, and links to other sites with active WebTrust seals.

The TruSecure[25] Enterprise Certification is another form of third-party review and is an integrated, continuous security program that addresses the most significant sources of risk across all the dimensions of an organization, providing security assurance in six major areas of risk: electronic threats and vulnerabilities, malicious code, privacy, physical security, and human factors. In the TruSecure Enterprise service, TruSecure analysts conduct a number of analyses of an organization's critical assets and locations. Additionally, the analysts visit a site to assess current risk levels and then work with network administrators over a period of time to create a customized program that meets the company's business and information security needs. TruSecure analysts repeat the electronic and on-site visits during the course of the program to ensure recommendations and mitigations have been applied. A Web-based console that ties into a proprietary database at TruSecure's Security Operations Center keeps track of compliance and creates a "Guidance Map" for security administrators to follow in the progress

[25]TruSecure is a security intelligence and service provider.

toward optimal risk reduction and ultimately, TruSecure Certification. We determined that Cendant, an FDIC contractor that services the FDIC Relocation Program through its system, Client Connect, completed an organizational risk assessment and received the TruSecure Enterprise Certification.

Moreover, pending legislation, the *Personal Data Privacy and Security Act of 2005* (S.1789), would amend FISMA, Section 3544(b), to require agencies to develop and implement procedures for evaluating and auditing the information security practices of contractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information and ensuring remedial action to address any significant deficiencies.

Some form of third-party security review would provide the FDIC independent assurance that contractor Web sites and systems contain adequate controls to protect the security, confidentiality, and privacy of FDIC personal employee information. Ideally, the Corporation could require, during the contract solicitation process, that qualified offerors obtain a third-party security review and maintain that designation throughout the term of the contract. Requiring a contractor to obtain a single security review that multiple federal agencies or other customers could rely upon would be a more reasonable approach than requiring multiple security reviews of a contractor by individual agencies. Requiring a third-party review would also place responsibility on the contractor for demonstrating that it has adequate Web site and system security.

Finally, Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/ Third Party Products*, does not address information security expectations and requirements for contractors that maintain Privacy Act or sensitive information (e.g., open bank or procurement sensitive information) but that are not directly connected to the FDIC's network. The circular also lacks encryption requirements for electronic transmissions to these contractors.

Recommendations

We recommend that the CPO:

13. Revise the PIA template and completed PIAs to include a question pertaining to the opportunities system users have to decline to provide information or to consent to particular uses of information and how system users may grant consent.

14. Research, including discussing with CIO counterparts from other agencies and the OMB, the feasibility, benefits, and costs of requiring that contractors and vendors who are not connected to the FDIC's network, but who maintain Privacy Act information on behalf of the FDIC, receive some form of third-party information technology security review.

15. Revise FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*, to include security expectations, including encryption requirements, for contractors and vendors that are not connected to the FDIC's network but maintain Privacy Act information on behalf of the FDIC.

MATTERS FOR FURTHER CONSIDERATION

Additional Initiatives Could Be Considered for Increasing Controls for Safeguarding Personal Employee Information

We identified several other controls that the FDIC could consider to further heighten awareness among corporate employees for safeguarding personal employee information entrusted to them.

File Clean-up Days: The FDIC's policy is that all sensitive records, regardless of where they are physically stored, must be destroyed by shredding, pulping, maceration (in the case of computer discs and CDs), or similar manner that prevents access to the information captured in the disposable files. In conforming to corporate policy, DOA's Corporate Services Records Management Unit installed secure shredding bins throughout headquarters offices to be used on an ongoing basis for disposal of sensitive and confidential material. The FDIC's off-site records storage vendor is responsible for periodically replacing full bins with empty bins and destroying the sensitive documents off-site. In addition, through the FDIC's national contract with the off-site records storage vendor, shredding bins are being used throughout the Dallas and Kansas City offices, including certain smaller area offices.

Government Security – The Risks and Costs of Inadequate Security

Did you know...

- Most information that is shared unwillingly is done so by leaving documents and computers unattended, even if only for a few minutes.
- Most trespassing incidents occur because offices do not keep their offices secured, neglect to regularly change access codes, or choose unrelated access codes each month.
- Most breaches of security occur during business hours while other people are present.

Source: Federal Lock & Safe, Inc. (FedLock).

In conjunction with these efforts, we suggested to DOA that it consider sponsoring a file clean-up day in preparation for the relocation of FDIC employees from various headquarters offices in downtown Washington, D.C., locations to the FDIC's Virginia Square complex scheduled to take place in early 2006. We envision a file clean-up day to be one wherein employees spend the day cleaning files, discarding records no longer needed, and preparing files and documents for disposal by shredding, pulping, or maceration as specified in the FDIC's policy. Future clean-up days could be scheduled periodically, as needed. DOA officials appeared receptive to this suggestion, especially in light of the pockets of unofficial personnel files -- such as employee folders maintained by supervisors -- that exist in the Corporation.

Clean Desk Policy and DOA Walk-Through Monitoring: In Evaluation Report No. 00-006, *FDIC's Information Handling Practices for Sensitive Employee Data*, dated October 11, 2000, we reported that the FDIC had procedures and practices in place that were designed to prevent unauthorized disclosure or access to records or systems to individuals without a business need to know. Included in the general practices was the FDIC's implementation of clean desk policies in some offices to help ensure that sensitive information was not inadvertently left unattended. HR officials told us that the clean desk policy was no longer being practiced in their respective groups, but said that other controls, such as limited access to work areas wherein personal employee information is being maintained, were still in place. We suggest that the FDIC encourage its corporate managers that routinely handle personal employee information to adopt the clean desk policy during non-working hours. We also suggest that DOA periodically perform walk-through inspections of its offices and work areas wherein personal employee

information is maintained in order to continually monitor the physical safeguards for protecting the sensitive data. For example, DOA representatives could make spot checks of copiers and telefax machines to determine whether documents containing sensitive information are being left unattended and observe the types of documents being discarded in trash cans to ensure that sensitive information is not included.

Sending Periodic Reminders to Regional Staff: In November 2004, the HR Associate Director, DOA, sent an electronic message to HR staff in headquarters regarding the protection of sensitive personnel information and the need to encrypt messages that contain sensitive information being sent to FDIC vendors. The message referenced and provided electronic links to the following:

- Circular 1310.5, which requires that individual division/office managers establish specific requirements regarding encrypting and digitally-signing electronic messages. The circular also states that electronic messages and attachments containing personnel related actions should be considered for encryption.
- FDIC guidance and instructions for digital signature and encryption.
- Circular 1031.1, which provides guidance to employees about the rights provided and the responsibilities imposed by the Privacy Act of 1974.
- OPM's *The Guide to Personnel Recordkeeping*, addresses, in part, security issues regarding the use of personnel records containing sensitive or private information.
- A list of the types of communications that HR staff have with potential employees, employees on board, OPM, and FDIC organizations, including recommendations for encryption when the information is sent through electronic messages.

We suggest that DOA periodically update and reissue the information from the November 2004 electronic message to HR staff in headquarters and regional offices to maintain awareness.

Informing Employees about the Availability of Security Tips: DIT's Web page and DOA's Security Management Section (SMS) Web page include links to *SECURITYsense*, a publication of the National Security Institute, Inc., an organization established in 1985, which provides a variety of professional information and security awareness services to the federal government and private industry. *SECURITYsense* is a monthly newsletter on information security that includes the latest exploits, vulnerabilities, and tips on using personal computers, personal data, and personal information. DIT subscribes to this newsletter. The following are examples of some of the topics discussed in the newsletters:

- *Identity Theft: Know the Warnings* (October 2005).
- *5 for the Road: Protect Your Laptop (and the Data Inside It)* (July 2005).
- *10 Data Security Tips for All Employees* (April 2005).
- *10 Ways to Work More Securely* (February 2005).
- *Q&A: How Vulnerable is Your Social Security Number?* (December 2004).
- *Five ID Theft Tips:* More Firms Guarding Employee Data (October 2004).
- *ID Theft and the Workplace: 5 Things You Need to Know* (June 2004).

The National Security Institute, Inc., suggests seven ways for subscribers to deliver *SECURITYsense* to employees:

1. Post each new issue on the company Web site.
2. Electronically mail the monthly contents page to all employees.

3. Publish articles in the company newsletter.
4. Make an attractive poster out of any of these quick-read stories.
5. Create handouts that will actually get read.
6. Reprint content for use in memoranda or bulletins.
7. Create a pop-up window that features an article or tip.

We suggest that the FDIC publicize to its employees and contractors the availability of *SECURITYsense* on its Web site and encourage employees and contractors to read the newsletters.

SMS Physical Security Inspections and Proprietary and Cipher Locks: In July 2005, SMS conducted a physical security assessment of DOA's Benefits Center and recommended that the Center discontinue using SSNs in its correspondence and consider adopting the clean desk policy for its operations. We encourage the FDIC to periodically remind its employees about the SMS' physical security vulnerability assessments and encourage those organizations that routinely handle personal employee information to request an SMS assessment.

Government Security – The Risks and Costs of Inadequate Security

Here are some security tips…

- Never leave classified or critical documents unsecured.
- Never leave your office or desk unsecured.
- Always change combinations on safe locks every year, without fail (it's the law for sensitive document storage).
- Always change combinations on safe locks any time the person who was the primary user of the safe leaves the organization.

Source: Federal Lock & Safe, Inc. (FedLock)

SMS officials also suggested that FDIC organizations handling personal employee information consider adopting the following best practices with respect to locking devices:

- Periodically change the codes in mechanical pushbutton (cipher/keypad) locks. Although not mandated to do so, SMS changes the codes in its keypad locks when an SMS employee leaves or every 6 months.
- Replace standard locks on file cabinets and desks with proprietary locks that have keys that cannot be reproduced. A key for a standard lock can be reproduced.

CORPORATION COMMENTS AND OIG EVALUATION

The Corporation provided a written response dated December 16, 2005 to a draft of this report. The Corporation's response is presented in Appendix VII (without attachments). The FDIC concurred with the intent of each recommendation and agreed to take corrective action on 12 of the 15 recommendations. For the remaining three recommendations (6, 10, and 11), the FDIC indicated, and we concur, that actions taken and/or controls already in place were sufficient and that no further action was warranted. These three recommendations are discussed in more detail below. The FDIC's written response also included supporting documentation sufficient to close three recommendations (4, 8, and 12). The remaining recommendations (1, 2, 3, 5, 7, 9, 13, 14, and 15) are resolved but will remain open until we have determined that agreed-to-corrective actions have been completed and are effective. Appendix VIII presents a summary of the Corporation's response and the status of each recommendation.

Recommendation 6 advised DOA, in conjunction with the Legal Division, to require contracts involving the electronic transmission of Privacy Act information to include encryption

requirements. DOA concurred with the intent of the recommendation but noted that the APM places responsibility with the program office to identify appropriate security requirements through the contract SOW. Thus, DOA believes the program office would be in the best position to identify whether encryption is necessary. DOA also noted that the APM requires contracts subject to Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/ Third Party Products*, to include IT security and monitoring requirements in the SOW. In response to recommendation 15, the CPO and DIT agreed to revise Circular 1360.17 to enhance guidance provided to contractors that are not connected to the FDIC's network but that maintain Privacy Act information on behalf of the FDIC. We consider DOA's response, along with DIT's plans to revise Circular 1360.17, sufficient to close the recommendation.

Recommendation 10 advised DOA to evaluate and determine whether DOA should adopt DSC's practice of not maintaining Unofficial Personnel Files or "working files" and consider establishing a corporate-wide policy consistent with that practice. DOA responded that it had evaluated its practices and decided to continue to maintain these files. DOA indicated that UPFs provide a means for employees and supervisors to readily access information on a regular basis and likely reduce the volume of requests for access to OPFs and, thus, reduce the possibility of compromising OPFs. DOA noted that it had complied with the notice requirements of the Privacy Act and that UPFs were adequately secured. DOA also indicated that it had considered the need for a corporate-wide policy, and determined that one was not needed at this time. While we continue to question the need for UPFs, DOA made a good faith effort to evaluate its practices and the need for a corporate-wide policy, and provided a sufficient basis for not taking corrective action. Therefore, we consider DOA's actions sufficient to close the recommendation.

Recommendation 11 advised DOA to develop corporate guidelines detailing appropriate job tasks that interns should perform and strengthen controls over interns' access to sensitive information. DOA concurred with the intent of the recommendation but responded that proper controls are in place over student and intern access to sensitive information. DOA noted that (1) all students and interns employed in HRB are required to complete FDIC's privacy awareness training, (2) supervisors are responsible for discussing the safeguarding of personal employee information with their students and interns and monitoring their use of encryption when sending personal employee information via e-mail, and (3) students and interns hired as year-round employees, as well as summer interns who return to work with the FDIC, undergo the same background investigations as other HRB employees. DOA also pointed out that the nature of tasks assigned to interns and students, such as opening mail, make it impossible to employ students and interns in HRB without exposing them to personal employee information. We encourage DOA to continue to seek opportunities to raise awareness and to limit students' and interns' access to personal information. However, the controls that DOA described in place over that access, if effectively implemented, appear to provide reasonable safeguards. Therefore, we consider management's response sufficient to close the recommendation.

Objective, Scope, and Methodology

We performed this evaluation at the request of the Director, DOA, who asked that the OIG evaluate the Corporation's procedures for handling personal employee information. This DOA request was in response to a security breach involving unauthorized access to personal information on a large number of current and former FDIC employees. The objective of our review was to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic forms. This evaluation does not address other types of confidential or sensitive information such as open bank, depositor, or procurement sensitive information.

We performed our evaluation from July 2005 through October 2005 in accordance with generally accepted government auditing standards. We performed field work in DOA, DIT, DOF, and the Legal Division located in Washington, D.C. In addition, we performed field work, in the Atlanta and Dallas DOA regional offices to evaluate the safeguards over maintaining and storing employee OPFs.

To accomplish our objective, we performed the following:

- Identified criteria used to establish the definition of personally identifiable information.
- Reviewed relevant criteria, including, but not limited to, the Privacy Act of 1974; E-Government Act of 2002; Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005; and OMB Circular No. A-130, *Management of Federal Information Resources,* Appendix I, *Federal Agency Responsibilities for Maintaining Records on Individuals*. Appendix II contains an overview of applicable laws and regulations.
- Reviewed privacy awareness information regarding the Risk Mitigation Project Team's recommendations to the CIO Council for safeguarding sensitive electronic information.
- Interviewed Legal Division's FOIA-Privacy Act Group to gain an understanding of the FDIC's long-standing privacy program and continued coordination efforts since appointment of the CPO, continuous efforts to publish and update the FDIC's SORNs, and efforts to perform OMB A-130 reviews of identified SORNs.
- Reviewed the FDIC Privacy Act SORNs that contained personal employee information.
- Reviewed the draft revised FDIC Privacy Act Circular and the Legal Division memorandum regarding roles and responsibilities of the CPO.
- Discussed the status of activities and initiatives related to development of a comprehensive privacy program for the Corporation.
- Reviewed the FDIC's PIA template and the PIA completed for CHRIS. Confirmed that PIAs had been completed on the 27 applications that DIT has identified thus far as containing sensitive personal information in order to meet FISMA reporting requirements.
- Obtained an overview from DOA's senior management of HR's policies, procedures, and practices for safeguarding personal employee information electronically and in hardcopy.
- Discussed HRB practices regarding safeguarding OPFs and other HR processing that involves personal employee information.
- Observed the operations of the Washington, D.C.; Atlanta; and Dallas OPF file rooms.
- Discussed policies, procedures, and practices for safeguarding personal employee information obtained through background investigations and other background checks, investigations of employee misconduct and performance problems, recruitment and career management services, and records management.

- Analyzed DOA's ASB practices relating to safeguarding personal employee information to which FDIC contractors and vendors have access and identified the specific contractors with access.
- Assessed encryption requirements for transmission of sensitive information from HRB to vendors and/or contractors.
- Assessed the FDIC's use of student interns involved in processes containing employee personal information and their access to sensitive information as well as the FDIC's risk designation for the intern position.
- Reviewed the FDIC APM to identify provisions related to confidentiality agreements and the Privacy Act and reviewed selected contract files to determine whether appropriate provisions and clauses related to privacy and confidentiality agreements were included.
- Assessed DIT's efforts to identify systems and applications containing personal employee information.
- Discussed the status of the SSN project and efforts to limit use or mask SSNs in existing applications.
- Met with OIG contractor, KPMG LLP, to discuss the FDIC's responses to the FISMA Section D questions relating to the privacy program.

Validity and Reliability of Performance Measures

We reviewed the FDIC's performance measures under the Government Performance and Results Act, the Corporate Performance Objectives (CPO), and the FDIC's annual performance plan (APP). We determined that the 2005 CPOs and APP did not include an initiative relating to its privacy program.

Reliability of Computer-based Data

We identified and relied on some computer-based data pertaining to the following systems that DOA, DOF, and DIT identified as containing personal employee information (CHRIS, NFC, Digital Library's CEFile, ARMS, and ETVPS). However, we did not test the reliability of computer-based data extracted from these automated systems because our evaluation objective did not require determining the reliability of computer-based data obtained from the systems.

Internal Controls

We gained an understanding of relevant control activities by reviewing (1) FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form, and (2) assessing FDIC's initiatives to enhance its privacy program. To gain this understanding, we interviewed the CPO, Privacy Program Manager, Privacy Act Clearance Officer, and individuals in DOA, DOF, DIT and the Legal Division involved in protecting and securing personal employee information. The finding sections of the report contain recommendations to strengthen certain policies and procedures, practices, and guidance.

Fraud and Illegal Acts

The nature of our evaluation objective did not require that we assess the potential for fraud and illegal acts. However, throughout the evaluation, we were alert to the potential for fraud and illegal acts, and no instances came to our attention.

Overview of Applicable Laws and Regulations Related to Privacy

Law	Description
Privacy Act of 1974	Provides specific guidance to federal agencies on the control and release of agency records that relate to individuals. The Act establishes safeguards for the protection of records the federal government collects and maintains on individuals.
E-Government Act of 2002	Establishes a broad framework of measures requiring use of Internet-based information technology to enhance citizen access to government information and increase citizen participation; improve government efficiency and reduce government costs; and promote interagency collaboration in providing electronic government services to citizens and the use of internal electronic government processes to improve efficiency and services provided. Section 208 of the Act includes procedures to ensure the privacy of personal information in electronic records, including agency preparation of PIAs relative to agency information systems.
The Federal Information Security Management Act of 2002 (FISMA)	Provides a comprehensive framework for agencies to secure federal information and assets. This Act is Title III of the E-Government Act of 2002.
Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005	Requires federal agencies to designate a CPO to carry out duties relating to privacy and protection of personal information collected and used by federal agencies. The requirements include safeguarding information systems from intrusions, unauthorized disclosures, and disruption or damage.
Paperwork Reduction Act of 1995	Generally requires federal agencies to manage information resources efficiently, effectively, and economically. The Act provides OMB with broad authority to oversee federal agency information resources and policy, including the privacy, confidentiality, security, disclosure, and sharing of information.
OMB Circular No. A-130	Establishes policies for federal agencies for the management of federal information resources, including automated information systems. Appendix I of the circular specifically covers agency responsibilities for implementing the reporting and publication requirements of the Privacy Act.

Responsibilities of the Chief Privacy Officer

General Policies	Reporting Requirements	Other Specific Tasks
• Overall agency responsibility for establishing, implementing, and administering privacy and data protection procedures and policies for personally identifiable information.	• Annual Report to the Congress on activities relating to privacy.	• Establish and implement comprehensive privacy and data protection procedures regarding the security of personally identifiable information.
• Ensuring that privacy is sustained, and not eroded, by new and emerging technologies relating to the use, collection, and disclosure of personally identifiable information.	• Privacy Impact Assessments.	• Prepare a written report for the Inspector General, signed by the CPO, of the FDIC's use of personally identifiable information, along with the established policies and procedures.
• Ensuring compliance with the Privacy Act, other privacy-related laws that apply to the FDIC, and established agency policies and procedures on privacy and data protection.	• Annual Report to OMB on security and privacy under FISMA.	• Ensure that an independent third-party review of the agency's privacy policies and practices is conducted at least every 2 years.
• Assisting in the design of employee training programs to promote awareness and compliance with the agency's established privacy policies.	• Biennial Report to OMB on computer matching.	• Post privacy policies on the FDIC's Web site.
• Overseeing, coordinating, and facilitating FDIC's compliance efforts and ensuring the Corporation's privacy procedures are comprehensive and up-to-date.	• Reports to OMB and the Congress on new or altered systems.	• Ensure that information that is retrievable by an individual identifier is collected, maintained, and protected to preclude unwarranted disclosure of personal information.
• Ensuring central policy-making role in the FDIC's development and evaluation of legislative, regulatory, and other policy proposals implicating information issues.		• Ensure that appropriate and adequate safeguards are established to protect records containing personally identifiable information from unauthorized access and disclosure.
		• Review agency Privacy Act training (every 2 years).
		• Review routine use disclosures for each system of records to ensure the recipient's use of records is compatible with the purpose for which the agency collects information (every 4 years).

Source: The FDIC's Legal Division Memorandum regarding *Responsibilities of the Chief Privacy Officer*.

Definitions for Privacy Act and Other Forms of Sensitive Information

FDIC Circular 1031.1 (Currently under revision.) ***The Privacy Act of 1974: Employee Rights and Responsibilities* (March 29, 1989)**
Circular cites the Privacy Act of 1974 definition of a "record" which is any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his or her education, financial transactions, medical history, and criminal or employment history and that contains his or her name, or the identifying number (such as a SSN), symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.
***OMB Guidance* for *Implementing the Privacy Provisions of the E-Government Act of 2002*, Attachment A, Section II.A.2**
Guidance includes the term "information in identifiable form," which is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, SSN or other identifying number or code, telephone number, e-mail address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.
DIT Guidance: *10 Tips to Protect IT Resources*
Guidance includes a non-exhaustive list of data and documents deemed to be "sensitive data." The list includes customer data, examination and enforcement data, legal documents, personnel data, assessment data, and resolutions and receivership data.
FDIC Circular 1310.5, *Encryption and Digital Signatures for Electronic Mail*
Guidance states e-mails and attachments that contain information of a private or sensitive nature that are transmitted over unsecured communications, such as the Internet, shall be encrypted and possibly include a digital signature. Email and attachments containing sensitive information such as personnel-related actions should be considered for encryption.
OPM Operating Manual: *The Guide to Personnel Record Keeping*
Manual defines the term "record" as all papers, maps, photographs, machine-readable materials or other documentation, regardless of physical form, made or received by the Government in connection with the transaction of public business and preserved as evidence of decisions, operations, or other activities of the Government. The manual states that the Privacy Act of 1974, as amended (5 U.S.C. 552a) applies to records under the control of an agency about an individual, such as an employment history, that contain the individual's name or some other item that identifies that person and from which information is retrieved by the name or other particular assigned to the individual. Agencies must ensure that personnel records subject to the Privacy Act are secured against unauthorized access. Access to personnel records subject to the Privacy Act should be limited to those whose official duties require such access. Agencies should establish procedures to allow employees or their designated representatives access to their own records. Agencies must ensure that those authorized to access personnel records subject to the Privacy Act understand how to apply the Act's restrictions on disclosing information from systems of records.
FDIC Web Privacy Guide
Guide cites personal information (or personally identifiable information) as any data that identifies an individual. Examples of personal information gathered from the definitions found in pending legislation are: name, e-mail address, home address, other physical address, telephone number, SSN, birth date, place of birth, birth certificate number, any other data that identifies an individual, and any other information that is maintained with, or can be searched or retrieved by means of, any other data in this list.
DIT Policy Memo, *Cookies in Internet Products*
Personal identifying information is defined for the purposes of Privacy Act issues in FDIC's Circular 1031.1, *The Privacy Act of 1974: Employees Rights and Responsibilities*. The following examples of personal identifying information have been gleaned from recent laws, regulations, and proposed legislation addressing online privacy: names, home and other physical addresses, telephone numbers, e-mail addresses, SSNs, any other identifier that permits the physical or online contacting of a specific individual, and any information that is maintained with, or can be searched or retrieved by means of data described in this definition.
***Guidance on Identifying Sensitive and Confidential Information* (Prepared by FDIC's Ethics Section)**
Guidance lists the general type of information that is considered to be sensitive and confidential information, regardless of whether the information is in a hardcopy document or an automated document and that may not be disclosed unless specifically authorized by law. The list includes employee personnel records that consist of all current and former FDIC employees and applicants to and graduates of the FDIC Upward Mobility Program. The guidance contains an extensive detailed list of information which may not be released including, for example, individuals' birth date, SSN, home address and telephone number, emergency contacts, employment and education experience, record of leave and time-and-attendance, performance appraisals; written notes or memoranda on employee performance; records relating to on-the-job training; data documenting reasons for personnel actions, decisions, or recommendations made about an employee; and documents related to on-the-job injuries.
FDIC Privacy Program Web site (external)
Web site references FDIC's Privacy Act regulations, which include the definition of a record as any item, collection, or grouping of information about an individual that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual. Web site also references personally identifiable information, information on individuals, and personal information, but does not provide a definition for these terms.

FDIC Systems of Records Containing Personal Employee Information

Number	Title	Location	Storage	Safeguards
30-64-0001	Attorney—Legal Intern Applicant Records	Legal Division	Paper format in individual file folders in cabinets	Records are maintained in lockable metal file cabinets accessible only by authorized personnel.
30-64-0003	Administrative and Personnel Action Records	Office of the Executive Secretary	Electronic media, microfilm, paper format within individual file folders, minute book ledgers, and index cards	Electronic files are password-protected and accessible only by authorized personnel. Paper format documents are stored in lockable metal file cabinets or vault accessible only by authorized personnel.
30-64-0006	Employee Confidential Financial Disclosure Records	Component divisions, offices, and regional offices.	Electronic media and paper format within individual file folders	Electronic files are password-protected and accessible only by authorized personnel. Paper format copies are maintained in lockable file cabinets.
30-64-0007	Employee Training Information Records	DOA	Electronic media and in paper format within individual file folders	Electronic files are password-protected and accessible only by authorized personnel. Paper records within individual file folders are maintained in lockable metal file cabinets accessible only by authorized personnel.
30-64-0010	Investigative Files of the Office of the Inspector General	OIG	Electronic media and paper format in individual file folders	Electronic files are password-protected and accessible only by authorized personnel and file folders are maintained in lockable file cabinets and lockable offices with access only by authorized personnel.
30-64-0011	Corporate Recruitment Tracking Records	DOA	Electronic media	Password protected and accessible only by authorized personnel. Network servers are located in a locked room with physical access limited to only authorized personnel.
30-64-0012	Financial Information Management Records	DOF Legal Division	Electronic media and paper format/record cards in individual file folders	Electronic files are password-protected and accessible only by authorized personnel. Paper documents are maintained in lockable metal file cabinets.
30-64-0015	Unofficial Personnel System	To be revised at a later date.	To be revised at a later date.	To be revised at a later date.
30-64-0017	Employee Medical and Health Assessment Records	Health Unit, Main Building, Virginia Square, and regions	Electronic media and paper format	Electronic files are password-protected. Paper format records are stored in lockable file cabinets with limited access.
30-64-0018	Grievance Records	DOA	Electronic media or paper format in individual files	Electronic files are password-protected. Paper records are stored in lockable file cabinets with limited access.
30-64-0020	Telephone Call Detail Records	DIT	Electronic media	Password-protected and accessible only by authorized personnel.
30-64-0021	Fitness Center Records	Fitness Center	Paper format within individual file folders	Records are kept in lockable file cabinets with limited access.

Source: FDIC Rules and Regulations, Part 310.

Types of Information Maintained in the Unofficial Personnel System SORN

Categories of Records in the System
1. **Information on Individuals** relating to: • Birth date, SSN, emergency contacts, addresses and telephone numbers. • Employment and education experience. • Original applications, résumés and letters of reference. • Record of material and equipment issued to individual. • Records of leave and time and attendance. • Performance appraisals, written notes or memoranda on employee performance, counseling. • Employee assignments, list of banks examined. • On-the-job training records. • Data documenting reasons for personnel actions, decisions, and recommendations made about the employee and disciplinary and adverse action backup material. • Claims for benefits under the Civil Service Retirement system. • Federal Employees Group Life Insurance and documents related to on-the-job injuries.
2. **Parking Permit Records** containing information (name, address, and type of automobile) about FDIC employees who have applied for a parking permit in the FDIC Washington office garage.
3. **FDIC Personnel Awards**, including information supporting the employee's nomination for one of these awards.
4. **Dental Insurance Records**, including information on earnings, number and name of dependents, sex, birth date, home address, and SSN.
5. **Employee Locator Records** containing employee's name, SSN, division or office assignment, office telephone number, and office room number.
6. **Upward Mobility Files** coordinated by the FDIC Office of Personnel Management.
7. **FDIC Savings Plan Records** containing the employee's name, SSN, grade, salary, home address, and birth date; record of employee contributions and FDIC contributions to investment funds, account earnings and balance; participant-designated beneficiaries; date of participation; indication as to whether a participant's interest is vested; allocation of contributions to investment funds; documentation for reason of hardship withdrawal and amount of withdrawal request (including documents evidencing purchase of primary residence, proposals to evict from, or foreclose on the mortgage of, a participant's primary residence, education expenses, medical expenses, and other acceptable financial hardship); documentation to support participation in the FDIC Savings Plan Loan Program; and personal financial statement.

Corporation Comments

FDIC
Federal Deposit Insurance Corporation

General Counsel
Division of Information Technology
Division of Administration

TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits

FROM: Michael E. Bartell [Electronically produced version; original signed by Michael E. Bartell]
Chief Privacy Officer (CPO),
Chief Information Officer (CIO), and
Director, Division of Information Technology (DIT)

Arleas Upton Kea [Electronically produced version; original signed by Arleas Upton Kea]
Director, Division of Administration (DOA)

William F. Kroener, III
General Counsel [Electronically produced version; original signed by William F. Kroener, III]

DATE: December 16, 2005

SUBJECT: Response to OIG Draft Report Entitled,
FDIC Safeguards Over Personal Employee Information
(Assignment No. 2005-048)

Thank you for the opportunity to respond to your draft audit report entitled *FDIC Safeguards Over Personal Employee Information*. We are commenting together on the various aspects of the draft report (rather than separately concerning issues within the scope of our respective divisions) because of the highly cross-divisional nature of all the issues involved and the importance of privacy matters to the Corporation in general.

We have carefully considered each of your 15 recommendations suggesting how the FDIC may further protect personal employee information. In summary, we concur with all 15 of the recommendations. Our full response to each recommendation is provided below.

Recommendation #1

That the CPO and General Counsel develop and issue an overarching privacy policy to include:

- coordination and reporting responsibilities and expectations among the CPO, the Privacy Act Clearance Officer and FOIA/Privacy Act staff, and SORN system managers;
- references to other relevant privacy and information security directives;
- key roles and responsibilities including SORN system manager responsibilities; and
- definitions for information subject to the Privacy Act and for other sensitive information terminology, such as "personally identifiable information," and "information in an identifiable form."

Response to Recommendation #1

We concur with this recommendation. Prior to the initiation of this audit, the FDIC had a November 30, 2005 target for completing the framework approach that would then be used to conduct the review and consolidation of existing privacy directives and policies. This information was reflected in the monthly Privacy Program status reports provided to the OIG audit team during fieldwork. The actual review of directives, policies, Web sites, etc. will be an extensive effort and require a large resource/time commitment. As such, the completion of the review and consolidation effort is expected by September 15, 2006. The resulting documentation will include:

- coordination and reporting responsibilities and expectations among the CPO, the Privacy Act Clearance Officer and FOIA/Privacy Act staff, and SORN system managers;
- references to other relevant privacy and information security directives;
- key roles and responsibilities including SORN system manager responsibilities; and
- definitions for information subject to the Privacy Act and for other sensitive information terminology, such as "personally identifiable information," and "information in an identifiable form."

While we recognize that the OIG has suggested that the FDIC Privacy Program Working Group accelerate their efforts to accomplish this review and consolidation effort by December 8, 2005, it is the FDIC's position that existing policy is sufficient to meet the intent of Section 522 until the comprehensive review is completed and an overarching privacy directive is drafted, if necessary. As such, current FDIC privacy policy already satisfies the Section 522 stipulation to have implemented comprehensive privacy and data protection procedures and strategies by December 8, 2005.

Recommendation #2

That the CPO and General Counsel revise and republish the SORN for the Unofficial Personnel System to include updated, accurate:

- information about records maintained;
- references to FDIC offices, system managers, and safeguards over information; and
- identification in the System Location section of information being maintained by contractors or vendors.

Response to Recommendation #2

We concur with the recommendation to revise and republish the System of Records notice for the Unofficial Personnel System (30-64-0015) as required by subsection (e)(4) of the Privacy Act of 1974 (5 U.S.C. § 552a). We are presently conducting a comprehensive review of the current Unofficial Personnel System notice to ensure that personal information is handled in full accord with privacy law and policy. This review will ensure the accuracy and completeness of the notice with particular emphasis on changes in technology, function, and organization that may have made the notice out of date. This review will also focus on routine use disclosures

under 5 U.S.C. 552a(b)(3) to ensure they continue to be necessary and compatible with the purpose for which the information was collected. A draft of the revised System of Records notice is expected by March 31, 2006. Subject to approval by the Board of Directors, it is expected that the revised System of Records notice will be published in the Federal Register by September 15, 2006, in accordance with the procedures in OMB Circular A-130, Appendix I.

Recommendation #3

That the CPO and General Counsel determine whether records detailed in the SORN for the Unofficial Personnel System should be republished as separate, individual systems of records.

Response to Recommendation #3

We concur with the recommendation to determine whether any group of records included as part of the current Unofficial Personnel System notice should be republished and managed as a separate system of records pursuant to subsection (e) of the Privacy Act of 1974 (5 U.S.C. § 552a). The scope of review for the current Unofficial Personnel System notice will include a thorough reexamination of the purposes, routine uses, and security requirements of each group of records covered by the notice. This review is designed to ensure that all groups of records are evaluated to determine whether they continue to be compatible and appropriately combined. A draft of any new System of Records notice(s) is expected by March 31, 2006. Upon approval by the Board of Directors, the revised System of Records notice will be published in the Federal Register in accordance with the procedures in OMB Circular A-130, Appendix I.

Recommendation #4

That the Director, DOA in conjunction with the General Counsel prepare a standard Privacy Act contract clause for use in all contracts involving Privacy Act information.

Response to Recommendation #4

We concur with the recommendation to prepare a standard Privacy Act contract clause for use in all contracts involving Privacy Act information. A standard Privacy Act clause has been developed in conjunction with the Legal Division and has been incorporated into our Standard Documents and the General Provisions. (See Attachment 1)

Recommendation #5

That the Director, DOA in conjunction with the General Counsel modify existing contracts discussed in this report to include specific references to the Privacy Act.

Response to Recommendation #5

We concur with the recommendation to modify existing contracts discussed in this report to include specific references to the Privacy Act. The DOA Acquisition Services Branch (ASB) is

working to modify the contracts and the following table lists each contract and its status:

Contract Number	Contractor or Vendor	Modify Contract to include Privacy Act Reference	Modify Contract to include Confidentiality Clause	Signed Confidentiality Agreement
0100054CDX	Benefits Allocation Service (BAS)—Flexible Cafeteria Benefits Program	N/A. Initially a part of Contract.	Completed	Completed
0100210CDX	VSP	Completed	Completed	Completed
0100209CDX	CIGNA	(*)	(*)	(*)
0100167CDX	Aon Consulting	Completed	Completed	Completed
0100211CDX	MetLife	In process	In process	In process
0100163CCD	Labat Anderson	N/A. Initially a part of Contract.	In process	In process
0000526CJ3	JHM	N/A. Initially a part of Contract.	In process	In process
0500029BCE	Contract Consultants	In process	In process	In process
0200004CPB	Ikon	In process	In process	N/A. Initially a part of contract.
0300091CVB	Cendant	In process	N/A. Initially a part of contract.	In process
0200133CJT	SatoTravel	N/A. Initially a part of Contract.	In process	In process
0200248CDQ	Impact Training Systems	In process	In process	In process
0100278CBK	Career Development Leadership Alliance	In process	In process	In process
N/A	T. Rowe Price (Trust Agreement)	In process	N/A. Initially a part of contract.	N/A
0400450TVB	NFC Interagency Agreement	N/A. Initially a part of Contract.	In process	N/A

* CIGNA's legal department reviewed these agreements and responded as follows: "With respect to the first part of the document entitled "Privacy Act," we can sign it. The legal group reviewed the relevant federal statutes and it is our position that we are not "required to design, develop, or operate a system of records on individuals to accomplish an FDIC function," within the meaning of the statute. Thus, signing the agreement has no effect on the underlying policy. With respect to the second part of the document entitled "Confidentiality Agreement," CIGNA cannot sign it. Paragraph 3.b. would prevent CIGNA from performing services for the FDIC. If signed, then every time information on an FDIC employee was transferred to one of our subsidiaries, affiliates or third party vendors, CIGNA would need to get something in writing from them agreeing to the terms in the confidentiality agreement. This would be considered as a separate agreement. The underlying policy is a filed and approved document by the state insurance department. Accordingly, it cannot be modified. This contract modification only modifies our agreement with the FDIC, but not the underlying policy." The FDIC Legal Division concurred with this interpretation and concurred in a modification to the standard form for CIGNA. As a health provider, CIGNA is bound by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the federal law that requires that they maintain the privacy of all patient medical and health information. The modification documentation was sent back to CIGNA for signature, but has not yet been received.

It is estimated that all contract modifications will be executed no later than January 31, 2006. The modifications will contain the newly developed Privacy Act and Confidentiality requirements as described in the response to recommendation 4 above.

Recommendation #6

That the Director, DOA in conjunction with the General Counsel require contracts which involve the electronic transmission of Privacy Act information to include encryption requirements.

Response to Recommendation #6

We concur with the recommendation that any Privacy Act information transmitted electronically should be encrypted. However, the ASB would not know the instances where Privacy Act information would be transmitted electronically between the FDIC and an outside contractor or the manner in which it should be transmitted. That requirement is best identified by the Program Office. Under the Acquisition Policy Manual, it is the responsibility of the Program Office to identify the appropriate security requirements through the Statement of Work (SOW). Further, the DOA Acquisition Policy Manual states that "IT security and monitoring requirements for contracts subject to Circular 1360.17 [Information Technology Security Guidance for FDIC Procurements/Third Parties, dated June 30, 2003] should be included in the SOW." Given that the CPO and DIT develop privacy and data protection policy, DOA will rely on the guidance of DIT in this matter. As these standards are developed and incorporated into a SOW, they would be incorporated into the contract.

Recommendation #7

That the Director, DOA require HRB and DOF contractors listed in this report to sign contractor confidentiality agreements.

Response to Recommendation #7

DOA management concurs with the recommendation and is working to modify the contracts identified by the OIG to include the confidentiality clause as referenced in the response to recommendation 4. Please see the table under recommendation 5 for the status of these contract modifications. DOA ASB anticipates all contract modifications to be signed no later than January 31, 2006.

Recommendation #8

That the Director, DOA remind contract specialists that they should not amend contracts or waive contractor confidentiality statement requirements without Legal Division concurrence.

Response to Recommendation #8

DOA management concurs with the recommendation. In the past few months, ASB has held several training/discussion sessions with the entire staff concerning the Acquisition Policy Manual. These sessions included training/discussion focused on this issue. Also, an email reminder was sent to contract specialists December 9, 2005. (See Attachment 2) DOA management considers this recommendation closed.

Recommendation #9

That the Director, DOA ensure that regional offices employ controls over official personnel files and any other personal employee information that are equivalent to those implemented by DOA's headquarters Human Resources Branch.

Response to Recommendation #9

DOA management concurs with this recommendation. The Human Resources Branch (HRB) will issue a memorandum to all Regional Offices by December 16, 2005 instructing the regions to: 1) specify in the SOW for the contractor-operated Official Personnel File (OPF) file rooms the tasks to be performed; 2) ensure that contractors sign confidentiality agreements; and 3) use the Automated Records Management System (ARMS) consistently to check OPFs in and out. (See Attachment 3)

However, Table 5 of the OIG's Draft Report cites an observation regarding the HRB's practice of transmitting the OPM Standard Form 75 (SF-75), *Request for Preliminary Employee Data,* by facsimile rather than by certified mail. The OIG noted that HRB officials had stated that sending SF-75s by certified mail to other agencies should be our practice. HRB management has since determined that the fax transmittal of these forms expedites the transmitting of employee information to other agencies as is preferred by these agencies. HRB, to ensure receipt, coordinates the sending and receiving of the SF-75 with the agency.

Recommendation #10

That the Director, DOA evaluate and determine whether DOA should adopt DSC's practice of not maintaining Unofficial Personnel Files or "working files" and consider establishing a corporate-wide policy consistent with that practice.

Response to Recommendation #10

DOA management has evaluated DSC's practice of not maintaining unofficial personnel files and the need for establishing a corporate-wide policy. DOA has determined to continue the practice of maintaining these Unofficial Personnel Files or "working files." DOA's administrative office in the Management Services Branch currently maintains working files on each employee within the DOA. These files contain a history of position descriptions, training authorization forms, emergency contacts, performance appraisals, SF-50s, and other documents. Employees often request access to their Unofficial Personnel File for various reasons. In addition, these files are included in the FDIC Privacy Act System of Records notice for the Unofficial Personnel System (30-64-0015) as required by the Privacy Act. The availability of the Unofficial Personnel Files would likely reduce the volume of requests for access to the OPF. In so doing, DOA reduces the possibility of compromising the OPFs and at the same time, provides a means for employees and supervisors to more efficiently and effectively access information needed on a regular basis.

From a security perspective, these files are held in a locked file cabinet inside a locked room and only the three administrative office personnel have access to the cabinet. The only people who may access an employee's file are these three administrative personnel, the employee, and his or her supervisor. The administrative personnel also maintain a log in/log out system that tracks file access.

Finally, DOA has considered whether or not a corporate-wide policy against the practice of maintaining Unofficial Personnel Files is needed and has determined that such a policy is not needed at this time. The subject of maintaining Unofficial Personnel Files is addressed under the current Bargaining Agreement and the Corporation has complied with the notice requirements of the Privacy Act.

Recommendation #11

That the Director, DOA develop corporate guidelines detailing appropriate job tasks that interns should perform and strengthen controls over interns' access to sensitive information.

Response to Recommendation #11

DOA management concurs that it is important to ensure that sensitive employee information is protected and we believe that proper controls are in place over student and intern access to sensitive information. All students and interns employed in the HRB participate in the Corporation's privacy awareness training. They receive the same annual notices as other employees to complete privacy awareness training and their completion of that training is monitored. Supervisors are responsible for discussing with their students and interns the safeguarding of personal employee information at the time they are hired. Their supervisor also instructs them on and monitors their use of encryption whenever they are sending personal employee information via e-mail. Further, students and interns who are hired as year-round employees do undergo the same background investigations to which all other employees in the HRB are subject. Only summer interns receive the less rigorous background check described in the recommendation. However, if a summer intern returns to the FDIC, he or she will undergo a full background investigation, as students who are on board for more than 180 days.

We wish to point out that it would be an impossible expectation to employ students and interns in HRB without exposing them to personal employee information. Even such routine activities as opening the mail often involve access to personal employee information. All HRB employees, including students and interns, are cautioned to maintain the confidentiality of employee data. Management considers this recommendation closed.

Recommendation #12

That the Director, DOA determine whether an employee identification number or other identifier could be used in place of employees' SSN in the Career Management Services' mentoring program database.

Response to Recommendation #12

DOA management concurs with this recommendation and eliminated the entry of employees' SSN in the Career Management Services' mentoring program database as of October 2005. All further databases transmitted to the contractor will use CHRIS identification numbers rather than SSNs. In addition, mentoring program applications for all future mentoring classes will request CHRIS identification numbers rather than SSNs from the applicants. Management considers this recommendation closed.

Recommendation #13

That the CPO revise the PIA template and completed PIAs to include a question pertaining to the opportunities system users have to decline to provide information or to consent to particular uses of information and how system users may grant consent.

Response to Recommendation #13

The CPO concurs with this recommendation and has completed the update to the Privacy Impact Assessment (PIA) template to include a question pertaining to the opportunities system users have to decline to provide information or to consent to particular uses of information and how system users may grant consent. Further, the CPO has begun to revise all existing PIAs to reflect this new requirement. All existing PIAs will be revised by April 15, 2006.

Recommendation #14

That the CPO research, including discussing with CIO counterparts from other agencies and the OMB, the feasibility, benefits, and costs of requiring that contractors and vendors who are not connected to FDIC's network, but who maintain Privacy Act information on behalf of the FDIC, receive some form of third-party information technology security review.

Response to Recommendation #14

The CPO concurs with this recommendation and will work in conjunction with DOA and Legal to research the feasibility, benefits, and costs of requiring that contractors and vendors who are not connected to FDIC's network, but who maintain Privacy Act information on behalf of the FDIC, receive some form of third-party information technology security review. This research and a report on the results will be completed by June 15, 2006.

Recommendation #15

That the CPO revise FDIC Circular 1360.17, *Information Technology Security Guidance for FDIC Procurements/Third Party Products*, to include security expectations, including encryption requirements, for contractors and vendors that are not connected to FDIC's network, but that maintain Privacy Act information on behalf of the FDIC.

Response to Recommendation #15

The CPO concurs with this recommendation and will enhance the security guidance provided to contractors and vendors that are not connected to FDIC's network but that maintain Privacy Act information on behalf of the FDIC. The enhancements will clarify what parts of the guidance apply to these types of contractors and vendors. FDIC Circular 1360.17 will be revised with these changes by September 15, 2006.

Attachments

cc: Ned Goldberg (DIT)
Tim Taylor (DIT)
Rack Campbell (DIT)
Dan Bendler (DOA)
Steve Hanas (Legal)
Fred Fisch (Legal)
James H. Angel, Jr. (OERM)

Management Response to Recommendations

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

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	The Corporation will conduct a comprehensive review of existing directives, policies, and Web sites and will develop and issue an overarching privacy policy, if necessary.	September 15, 2006	$0	Yes	Open
2	The Corporation is conducting a comprehensive review of the current UPS SORN to ensure that personal information is handled in full accord with privacy law and policy. A draft of the revised SORN will be prepared and will be subject to approval by the Board of Directors prior to publication in the *Federal Register*.	Preparation of draft SORN by March 31, 2006. Publication in the *Federal Register* by September 15, 2006.	$0	Yes	Open
3	The Corporation is conducting a review of the current UPS SORN, which will include a thorough reexamination of the purposes, routine uses, and security requirements of each group of records covered by the SORN. The review is designed to ensure that all groups of records are evaluated to determine whether they continue to be compatible and appropriately combined. A draft of any new SORN(s) will be prepared, if determined by the review.	Draft of new SORN, if necessary, by March 31, 2006	$0	Yes	Open
4	DOA, in conjunction with the Legal Division, has developed a standard Privacy Act contract clause and has incorporated the clause into its Standard Documents and the General Provisions.	Completed	$0	Yes	Closed
5	ASB will modify the existing contracts discussed in this report. The modifications will contain the newly developed Privacy Act and confidentiality requirements.	January 31, 2006	$0	Yes	Open

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
6	DOA concurred with intent of the recommendation but indicated that the program office was in the best position to identify those contracts with encryption requirements and noted that the APM requires contractors subject to Circular 1360.17 to include IT security and monitoring requirements in the SOW.	Not Applicable	$0	Yes	Closed
7	DOA will modify the contracts identified in this report to include confidentiality clauses.	January 31, 2006	$0	Yes	Open
8	ASB held several training/discussion sessions with ASB staff and issued an e-mail reminder that contract specialists do not have the authority to waive confidentiality statement requirements without the Legal Division's concurrence.	Completed	$0	Yes	Closed
9	HRB will issue a memorandum to all regional offices instructing the regions to: (1) specify in the SOW for the contractor-operated OPF file rooms the tasks to be performed; (2) ensure that contractors sign confidentiality agreements; and (3) use the ARMS to consistently check OPFs in and out.	December 16, 2005	$0	Yes	Open
10	DOA management evaluated DSC's practice of not maintaining UPFs and the need for establishing a corporate-wide policy. DOA determined a need to continue maintaining these files and that a corporate-wide policy was not needed at this time.	Not Applicable	$0	Yes	Closed
11	DOA concurred with the intent of the recommendation but responded that proper controls are in place over student and intern access to sensitive information. DOA's written response detailed examples of those controls.	Not Applicable	$0	Yes	Closed
12	DOA eliminated the entry of employees' SSNs in the Career Management Services' mentoring program database as of October 2005. All further databases transmitted to the contractor will use the CHRIS identification numbers rather than the SSNs. In addition, mentoring program applications for all future mentoring classes will request CHRIS identification numbers rather than SSNs from the applicants.	Completed	$0	Yes	Closed

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
13	The CPO has revised the PIA template to include a question pertaining to the opportunities system users have to decline to provide information or to consent to particular uses of information and how system users may grant consent. The CPO will revise all existing PIAs to include this question.	April 15, 2006	$0	Yes	Open
14	The CPO will work in conjunction with DOA and the Legal Division to research and document in a report the feasibility, benefits, and costs of requiring that contractors and vendors who are not connected to FDIC's network, but who maintain Privacy Act information on behalf of the FDIC, receive some form of third-party information technology security review.	June 15, 2006	$0	Yes	Open
15	The CPO will enhance the security guidance provided to contractors and vendors that are not connected to FDIC's network but that maintain Privacy Act information on behalf of the FDIC. The enhancements will clarify which parts of the guidance apply to these types of contractors and vendors and will be reflected in FDIC Circular 1360.17.	September 15, 2006	$0	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the OIG determines that agreed-to corrective actions have been completed and are effective, the recommendation can be closed.