Office of Inspector General

September 2006
Report No. 06-017

DRR's Protection of Bank Employee and Customer Personally Identifiable Information

Office of Audits

OIG

Office of Audits

Report No. 06-017
September 2006

DRR's Protection of Bank Employee and Customer Personally Identifiable Information

Background and Purpose of Audit

The FDIC's Division of Resolutions and Receiverships (DRR) has primary responsibility for resolving failed FDIC-insured depository institutions promptly, efficiently, and responsively in order to maintain public confidence in the nation's financial system. In performing their duties, DRR personnel have access to a wide variety of records containing personally identifiable information of a bank's employees and customers. The adequacy of DRR's controls over such information has become more important with the increased attention on the issue of identify theft.

The overall objective of the audit was to determine whether DRR adequately protects personally identifiable information collected and maintained as a result of resolution and receivership functions. We focused our attention on DRR efforts to protect information maintained in hardcopy form. We intend to conduct a future audit that more fully addresses DRR's controls over personally identifiable information in electronic form.

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

Results of Audit

Overall, through various policies and procedures, DRR has established certain controls over the resolution and receivership process addressing the protection of sensitive bank employee and customer personally identifiable information. Among the policies and procedures is DRR's *Failed Financial Institution Closing Manual*, which identifies the responsibilities of key DRR officials and highlights certain important controls for securing and establishing accountability for sensitive information. During our review of documentation supporting the four most recent institution closings, we found that DRR had implemented the controls as designed.

However, given the increased risks associated with, and attention being placed on, identity theft, we identified opportunities for DRR to strengthen controls over its handling of sensitive bank employee and customer personally identifiable information obtained during the resolution and receivership process. In particular, DRR had not established a Records Management Program that defines recordkeeping requirements for the inventory, maintenance, control, and use of hardcopy documents. As a result, personally identifiable information could be at increased risk of compromise or unauthorized use.

Further, other matters came to our attention during the audit relating to the FDIC's contract with Iron Mountain, Inc. for off-site records storage and the FDIC's overall Records Management Program administered by the Division of Administration (DOA). We provided these matters for DOA consideration in its current effort to draft an FDIC records management manual.

Recommendation

The report recommends that DRR work with DOA, and other cognizant FDIC divisions and offices, in developing a DRR Records Management Program that would include guidelines for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions. DRR management concurred with the recommendation and is forming a working group, which, in consultation with DOA and others, will develop records management guidance specific to their needs.

With regard to the other matters discussed in the report, DOA management indicated it is taking appropriate actions to address issues associated with the Iron Mountain, Inc. contract. Additionally, DOA will evaluate our information regarding the overall Records Management Program as the division continues to improve the program.

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

Office of Audits
Office of Inspector General

DATE: September 15, 2006

MEMORANDUM TO: Mitchell L. Glassman, Director
Division of Resolutions and Receiverships

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: *DRR's Protection of Bank Employee and Customer Personally Identifiable Information*
(Report No. 06-017)

This report presents the results of the Office of Inspector General's (OIG) audit of the Division of Resolutions and Receiverships' (DRR) efforts to protect bank employee and customer personal information obtained during the resolution and receivership process. When resolving failed institutions, DRR collects and maintains, in both hardcopy and electronic format, sensitive bank employee and customer personal information (hereafter referred to as personally identifiable information), and it is DRR's responsibility to protect such information.[1]

The overall objective of the audit was to determine whether DRR adequately protects personally identifiable information collected and maintained as a result of resolution and receivership functions. We focused our attention on DRR efforts to protect personally identifiable information maintained in hardcopy form. We limited our review of DRR's protection of personally identifiable information in electronic form to DRR's completion of risk assessments associated with systems containing personally identifiable information. We intend to conduct a future audit that more fully addresses controls over personally identifiable information in electronic form. Additional details on our objective, scope, and methodology are in Appendix I.

[1] The Privacy Act of 1974 protects "records" of individuals from unauthorized release by federal agencies. Records are documents that contain information about the individual regarding "his education, financial transactions, medical history, and criminal or employment history and that contain his name or identifying number." Subsequent legislation and regulatory guidance have built upon the Privacy Act's notion of personally identifiable information. For example, the E-Government Act of 2002 uses the phrase information in "identifiable form," which means information that permits the identity of the individual to be reasonably inferred, directly or indirectly. Further, on July 12, 2006, the Office of Management and Budget (OMB) issued Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, which includes an expanded definition of personally identifiable information. For purposes of this audit, we have relied on the Privacy Act and the E-Government Act's definitions, as well as OMB guidance relative to those statutes. Our audit report does not address the expanded definition in the recent OMB directive.

BACKGROUND

Within the FDIC, DRR has the primary responsibility for resolving failing FDIC-insured depository institutions promptly, efficiently, and responsively in order to maintain public confidence in the nation's financial system. In performing their duties, DRR personnel have access to a wide variety of records containing personally identifiable information of a bank's employees and customers. Such records include: bank employee payroll records, customer deposit records, and customer loan records.

DRR's Bank Resolution Process

DRR's *Failed Financial Institution Closing Manual* (Closing Manual) contains procedures for closing an FDIC-insured financial institution when the institution is placed into receivership. Although the Closing Manual is not intended to provide detailed, technical explanations of tasks to be performed (such detail is contained in other FDIC manuals and directives), the Closing Manual does provide closing procedures and guidelines for each program area participating in the closing. Based on the Closing Manual, other manuals and directives, and interviews with DRR officials, the summary below briefly outlines DRR's bank resolution process and provides a general overview of the types of bank employee and customer personally identifiable information that may come into DRR's possession both during and after the closing of a failing FDIC-insured institution.

- At the outset of the resolution process, DRR's Business Information Systems Section (BIS) receives a download of an institution's electronic records from either the failing institution's computer system or its data processing servicer, if one was used. Generally, this download consists of loan files, deposit account files, employee personnel files, and accounting files and may contain such bank employee and customer personally identifiable information such as name, address, Social Security number (SSN), and account number and balance. BIS makes this information available to other DRR operating groups that use the information to carry out closing-related tasks. (Other DRR operating groups include: Institution Sales, Asset Sales, Claims, Investigations, and General Accounting.)

- From the download, DRR's Pro Forma Team[2] creates a closing trial balance consisting of all the institution's assets and liabilities passing on to the FDIC in its capacity as receiver. This trial balance becomes the beginning inventory of the resulting receivership.

- DRR Institution Sales personnel use the downloaded data to establish estimates of the values of the institution's franchise and its assets for marketing purposes. In performing this work, Institution Sales may share bank information with prospective bidders of the bank franchise and any contractor that may be assisting with the sale.

[2] DRR's Pro Forma Team is comprised of the Financial Manager, Pro Forma Team Leader, Pro Forma support staff, and a tax specialist. The purpose of the Pro Forma Team is to produce an accurate adjusted Statement of Condition of the failed institution.

- DRR's Asset Sales, Claims, Investigations, and General Accounting groups work with the bank records in both hardcopy and electronic format to carry out closing-related responsibilities. Records that are needed for DRR's ongoing resolution process (such as loan files and employee records) are shipped to the Dallas Regional Office where they are stored until no longer needed. As with Institution Sales, Asset Sales may share certain bank information with potential purchasers when conducting resolution-related work.

Federal Laws and Guidance Related to the Protection of Personally Identifiable Information

The primary statute that regulates the federal government use of personally identifiable information is the Privacy Act of 1974. The Privacy Act covers a broad range of privacy-related issues, but there are two elements that apply specifically to our audit objective. The FDIC, according to the Act, is responsible for (1) maintaining in its systems of records only such information necessary and relevant to the function the Corporation is required to perform either by statute or by executive order of the President and (2) establishing reasonable administrative, technical, and physical safeguards to assure that records are disclosed only to those who are authorized to have access.

The Privacy Act has been augmented by a number of other laws, regulations, and guidance, including the E-Government Act of 2002, which includes the Federal Information Security Management Act of 2002 (FISMA); Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Section 522);[3] OMB Circular No. A-130, *Management of Federal Information Resources*, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*; and OMB's Memorandum, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*. These laws and regulations require government agencies to enhance and, in several cases, report on their privacy programs.

The E-Government Act of 2002 provides protection for personally identifiable information in government information systems or information collections by requiring that agencies conduct Privacy Impact Assessments (PIA).[4] In general, agencies must conduct a PIA before (1) developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form or (2) initiating any new electronic data collections containing personal information on 10 or more individuals other than federal employees and agencies. Among other actions that should require a PIA, according to guidance from OMB, is the significant merging of information in databases, for example, in a linking that "may aggregate data in ways that create privacy concerns not previously at issue" or "when agencies systematically

[3] This Act is division H of the Consolidated Appropriations Act, 2005.

[4] The E-Government Act defines a PIA as "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."

incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources." Bank employee and customer information that DRR collects during the resolution and receivership process falls into this category of information.

Appendix II further describes the laws and regulations applicable to DRR's protection of personally identifiable information.

Federal guidance related to records management has been promulgated by the National Archives and Records Administration (NARA).[5] Specifically, NARA publishes handbooks, conducts workshops and other training sessions, and furnishes information and guidance to federal agencies about the creation of records, their maintenance and use, and their disposition. Agencies, in turn, must institute adequate records management controls over the maintenance and use of records wherever they are located to ensure that all records, regardless of format or medium, are organized, classified, and described to promote their accessibility and are available for use by all appropriate agency staff for their authorized retention period. Agencies must ensure that they maintain adequate information about their records moved to an off-site records storage facility. Also, agencies must ensure the proper, authorized disposition of their records and must periodically evaluate records management programs.

FDIC's Records Management Program and Efforts to Address the Protection of Personally Identifiable Information

The FDIC's Division of Administration (DOA) administers a corporate-wide Records Management Program and, as a matter of policy, complies with the policies and procedures promulgated by NARA. DOA records management policies and procedures apply to all FDIC divisions and offices and govern the management of records created in the course of conducting business and records received by the FDIC from failed financial institutions. DOA facilitates the records disposition and storage process through its Records Management Unit and designates division and office Records Liaisons to cooperate with the DOA Records Manager serving their respective geographic locations.

For active records, FDIC operating divisions, such as DRR, are required to develop their own policies and procedures regarding inventory, handling, and storage practices. Additionally, according to FDIC Circular 1210.18, *FDIC Records Management Program*:

> Division and Office Directors shall support the FDIC Records Management Program as follows: (1) designate a records liaison who shall work with appropriate Records Manager in implementing policies and procedures; (2) promote the creation of adequate documentation throughout their organization

[5] Under the National Archives and Records Administration Act of 1984, NARA is responsible for promulgating records management regulations related to the adequacy of documentation and records disposition. The Act and regulations promulgated thereunder are not legally binding on the FDIC, but the FDIC intends to follow them as a matter of policy.

by defining the recordkeeping requirements for their programs in procedural manuals or other documentation. Recordkeeping requirements define the kinds of records each division or office should create and maintain to document their business activities; and (3) establish records management programs within their organizations that are consistent with FDIC policy and executed by division and office staff.

In accordance with Section 522, in March 2005, the FDIC appointed a Chief Privacy Officer (CPO), within the Division of Information Technology (DIT), 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 objective of the Privacy Program is to ensure that the FDIC is taking appropriate steps to protect personally identifiable information from unauthorized use, access, disclosure, or sharing and to protect associated information systems from unauthorized access, modification, disruption, or destruction.

The FDIC has issued a wide range of guidance to its employees on privacy-related matters. Specifically, DIT has issued a series of e-mails corporate-wide related to privacy and has established a Privacy Program Web site to assist employees in understanding the Privacy Act and the privacy policies of the Corporation. Further, as part of establishing a security program, the FDIC has developed and implemented several security-related directives. The following are most applicable to the protection of personally identifiable information:

- FDIC Circular 1031.1 – *Administration of the Privacy Act*.
- FDIC Circular 1301.3 – *Data Stewardship Program*.
- FDIC Circular 1310.3 – *Information Technology Security Risk Management Program*.
- FDIC Circular 1360.1 – *Automated Information Systems (AIS) Security Program*.
- FDIC Circular 1360.8 – *Information Security Categorization*.
- FDIC Circular 1360.15 – *Access Control for Automated Information Systems*.

The circulars are summarized in Appendix II. As discussed previously, our audit did not focus on controls over personally identifiable information in electronic form and related information technology controls.

RESULTS OF AUDIT

Overall, through various policies and procedures, DRR has established certain controls over the resolution and receivership process, addressing the protection of bank employee and customer personally identifiable information. Among the policies and procedures is the DRR Closing Manual, which identifies the responsibilities of key DRR officials and highlights certain important controls for securing and establishing accountability for sensitive information that is collected and maintained during the resolution and receivership process. During our review of documentation supporting the four most recent institution closings,[6] we found that DRR had implemented the controls as designed.

However, given the increased risks associated with, and attention being placed on, identity theft, we found opportunities for DRR to strengthen controls over its handling of bank employee and customer personally identifiable information obtained during the resolution and receivership process.

- DRR has not established a Records Management Program that clearly defines recordkeeping requirements for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions. Specific recordkeeping practices used by various DRR operating groups differed based on business needs and other circumstances but, in most cases, were not fully adequate. Further, in a broader view, DRR employees may not be sufficiently aware of division-specific recordkeeping requirements, including those designed to ensure that personally identifiable information is adequately secured. As a result, personally identifiable information could be at increased risk of compromise and unauthorized use **(DRR's Records Management Program and Controls over Hardcopy Documents)**.

- When we began our audit field work, DRR had not completed PIAs on certain systems containing personally identifiable information because DIT had initially identified only those systems containing Taxpayer Identification Numbers (TIN) as requiring PIAs. As a result, DRR had not ensured that privacy protections and Privacy Act requirements were fully considered for DRR systems containing personally identifiable information. However, based on our audit work, DRR took prompt action to assess the need for and, when necessary, to complete PIAs on additional DRR systems **(Privacy Impact Assessments)**.

Finally, other matters came to our attention during the audit relating to the FDIC's contract with Iron Mountain, Inc. (Iron Mountain) for off-site records storage and the FDIC's overall Records Management Program administered by DOA. With respect to the Iron Mountain contract, we found that improvements to certain key controls would increase assurance that Iron Mountain adequately protects the confidentiality of personally identifiable information and better protect the Corporation's interests should a breach of such information occur. Regarding the FDIC's Records Management Program,

[6] The closings occurred from February 14, 2004 to June 25, 2004.

DOA could assess the adequacy of the program and consider whether: sufficient attention is given to the management of active records, records management training should be strengthened, and corporate evaluations of the effectiveness of the Records Management Program are adequate.

DRR'S RECORDS MANAGEMENT PROGRAM AND CONTROLS OVER HARDCOPY DOCUMENTS

DRR policies and procedures establish controls over the resolution and receivership process addressing the custody of records containing bank employee and customer personally identifiable information. However, DRR has not established a Records Management Program that clearly defines recordkeeping requirements for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions. Further, the adequacy of the practices for handling hardcopy documents containing bank employee and customer personally identifiable information varied within five DRR operating groups. As a result, documents containing sensitive information under DRR's control were at greater risk to possible compromise and unauthorized use.

Records Management Program

FDIC Circular 1210.18 requires division and office directors to support the FDIC Records Management Program by "Establish[ing] records management programs within their organizations that are consistent with FDIC policy and executed by division and office staff." DRR has designated a records liaison as required by the circular and has issued some guidance in the area of records management, covering such topics as: (1) protecting borrower identity, (2) requests by debtors for copies of loan-related documents, and (3) information systems security responsibilities. However, DRR has not developed a records management program unique to its business needs to manage records and ensure records security.

Circular 1210.18 generally states that FDIC divisions and offices should establish the following recordkeeping requirements:

- Documentation of important business decisions reached orally during telephone conversations or in meetings.

- Documentation on formal meetings of committees and task forces that include the materials distributed, decisions reached, and subsequent actions.

- Working files such as preliminary drafts, rough notes, and other similar materials, which shall be maintained for the purpose of adequate and proper documentation if such materials (1) were circulated or made available to employees, other than the creator, for official purposes such as approval, comment, action, recommendation, or follow-up or to communicate with agency staff about agency

business; or (2) contain unique information, such as substantive annotations or comments, that adds to a sufficient understanding of the FDIC's formulation and execution of policies, decisions, actions, or responsibilities.

- Provisions in FDIC contracts requiring the contractor to provide any program or administrative documentation needed by the FDIC for effective management and for documenting the work performed by a vendor.

Further, the circular requires FDIC employees to ensure that their files are complete and accessible only to authorized individuals by implementing division or office guidelines for securing confidential information.

In developing guidance for its staff regarding records management, DRR could consider guidance issued by the Division of Finance (DOF) in a memorandum entitled, *Managing DOF's Confidential Records*, dated August 15, 2005. The guidance provided all DOF employees with (1) a definition of confidential records; (2) descriptive examples of what would constitute confidential records; and (3) general guidelines on managing confidential records, including such practices as maintaining records in locked areas and routing documents in sealed folders.

DRR Controls Over Hardcopy Documents

DRR is the custodian of records taken from a failed financial institution at closing as well as records generated during the resolution process. As custodian, DRR is responsible for properly managing these failed institution records. This responsibility encompasses all managerial activities involved with respect to the creation, inventory, maintenance, use, and disposition of the records. Of particular concern to us during this audit was DRR's inventorying, handling, storing, and disposing of failed institution records containing personally identifiable information.

Controls Over Hardcopy Documents DRR Obtained and Generated at Closings. The institution closing files developed for each of the four failed institutions we reviewed contained evidence that DRR maintained adequate custody over bank records (including loan, collateral, payroll, and personnel files). Specifically, the closing files included: (1) a written record of the FDIC's appointment as receiver of the failed institution; (2) if pertinent, a receipt and inventory of items passed on to an assuming institution; and (3) a detailed listing of the institution's hardcopy records kept by the FDIC which were primarily loan files, investigation records, and employee records. The closing files also included exit memorandums, signed by the cognizant DRR managers, which discussed the services closing teams performed and any issues dealt with during the closing process. However, DRR was not always using the FDIC's Automated Records Management System (ARMS) for the active asset/credit files of the failed institutions, as required by Circular 1210.18. We found that only DRR's Investigations group used ARMS as an inventory for active records.

Controls Over Hardcopy Documents That DRR Maintains. We assessed each DRR operating group's controls over hardcopy institution documentation in their possession at the time of our audit. We specifically determined whether the groups were: (1) keeping records in locked file cabinets, (2) storing records in locked file rooms, (3) using sign-out sheets when records are removed, and (4) maintaining an inventory of hardcopy records. The following table summarizes our assessment of these controls and shows that the adequacy of the control processes varied among the groups.

Hardcopy Document Handling and Storage

Group	Locked File Cabinets	Locked File Room	Sign-out Sheets	Inventory of Active Records
Institution Sales	Yes	Yes	Yes	N/A
Asset Sales	Yes/No[a]	Yes	No	Yes
Claims	Yes	Yes	No	Yes
Investigations	No	Yes	No	Yes
General Accounting	No	No[b]	No	N/A

Source: OIG's observations and assessment of each group's practices.
[a] Asset Sales secured the original loan notes and collateral documents in locked file cabinets; however, other documentation was not secured in locked file cabinets.
[b] Initially, General Accounting did not secure tax documents and related computer equipment. After our visit, steps were taken to place locks on records storage rooms.

We recognize that general FDIC security in the Dallas Regional Office includes employee screening, controlled floor access using Smartcard, and building security personnel who guard the building's main entrances and monitor the floors. We believe, however, that more could be done to ensure adequate control over personally identifiable information as discussed in the following narrative.

Hardcopy Document Handling and Storage by Institution Sales. DRR Institution Sales personnel use information acquired from the BIS electronic download of the bank's computer system to prepare Information Packages (IP) and to perform Asset Valuation Reviews (AVR) for valuing and marketing the institution franchise. They remove no hardcopy records from the failing bank. During the marketing phase of DRR's structured bidder selection process, approved bidders have access to selected bank information online through a secure Web site, INTRALINKS.[7] Bidders also have the opportunity to perform due diligence of the hardcopy loan files on-site at the bank. With respect to these activities, DRR has issued Circular 7220.5, *Protecting Borrower Identity*, which states:

> The FDIC will not disclose within databases, lists or spreadsheet summaries the names, addresses or social security numbers ("Identity Information") of individuals who are borrowers or guarantors to prospective purchasers without

[7] INTRALINKS is a private Internet-based company DRR engaged to assist in the marketing of failing institutions. The purpose of establishing a secure Web site is to provide information in an expeditious manner on failing financial institutions to potential acquirers.

first, (i) obtaining an executed or assented to FDIC Confidentiality Agreement[8] in accordance with the terms of the sale, and (ii) determining that prospective purchaser meets the requirements of Paragraph 5 of this circular.

Institution Sales developed procedures and a job aid instructing its employees about how to oversee the due diligence process. These instructions include: (1) requiring that two DRR employees be in attendance at all times and (2) prohibiting prospective bidders from making copies of any institution records. It should be noted that with respect to on-site bidder due diligence, DRR has made a business decision to allow bidders to review files that could contain personally identifiable information, such as name, address, SSN, and account number.

During our walk-through of the Institution Sales offices in Dallas, Texas, we observed elements of their controls over hardcopy documents. Specifically, we noted that the internal working documents created from the BIS data for the IP and AVR were stored in locked file cabinets, inside a secure file room. According to Institution Sales officials in Dallas, three people control access to this secured file room. Further, Institution Sales maintained a sign-out sheet in the file room, requiring that personnel needing to work on a particular file sign for the file. We found recent activity on the sign-out sheet, thereby providing at least some indication that it was being used.

Because Institution Sales does not remove individual loan files or any other hardcopy records from the failed bank, a detailed inventory of employee or customer records under its control is not maintained. However, the group does maintain a folder that lists the internal working documents created from the BIS download and used during IP and AVR efforts.

Hardcopy Document Handling and Storage by Asset Sales. DRR Asset Sales is responsible for selling a bank's assets after closure, and Asset Sales personnel are subject to the same policies and job aids as Institution Sales. The original loan notes and collateral documents are reviewed at the bank and reconciled with the bank's records. The asset sales process includes a due diligence phase that is similar to due diligence performed during the marketing phase of the bidder selection process. The major difference is that the due diligence occurs at the FDIC's Regional Office in Dallas, Texas, as opposed to on-site at the failed institution. Potential bidders are screened and must sign confidentiality agreements.

Unlike Institution Sales, Asset Sales takes hardcopy records such as original loan and collateral files from the failed financial institution. Asset Sales reconciles these files to the loans on the books of the institution at the closing. This reconciliation is accomplished before the files are shipped to the Dallas Regional Office. The resulting loan trial balance becomes the inventory of assets, and a copy of this inventory is placed in a Closing Manager's Book. Asset Sales maintains the hardcopy records in a locked

[8] Confidentiality agreements are executed documents whereby a contractor or third party must ensure the confidentiality of all the information, data, and systems provided by the FDIC or used or obtained by others under the agreement and prevent its inappropriate or unauthorized use or disclosure.

file room. The original loan and collateral documents are further secured in locked file cabinets inside the locked room, while other asset files are in unlocked file cabinets inside the locked file room. Therefore, the other asset files were at a somewhat greater risk of possible misuse.

Hardcopy Document Handling and Storage by Claims. DRR Claims primarily deals with a failed bank's deposit information and is responsible for determining the insured and uninsured deposit amounts. Claims starts with the BIS electronic data download from the bank and, although Claims personnel do not remove any bank records from the failed financial institution at closing, the working files generated to support the claims process do contain personally identifiable information regarding customers' deposit accounts. Deposit information is loaded into the Receivership Liability System (RLS), and the deposit information in RLS becomes the Claims inventory. All hardcopy documents generated from the electronic records are locked in file cabinets and stored inside a secure file room. The file room remains open during the day. Although there is no sign-out sheet for the file room, the sign-out card for files has to be placed in the file drawer when files are removed.

On March 31, 2005, Claims management issued a memorandum to all Claims personnel, establishing standard procedures for the security of system-generated (printed) products from RLS. The guidance states that if no longer required to be maintained, sensitive printed documents are to be placed in locked containers for shredding. Further, the guidance states that sensitive printed data and other storage media documents are not to be left out or in open common areas such as conference rooms and that at night (after normal working hours), such documents are to be placed in the claims specialists' offices or Claims' file room.

Hardcopy Document Handling and Storage by Investigations. Personnel from DRR Investigations retrieve a wide variety of hardcopy documents during a bank closing. These documents include corporate charters, stock certificates, board meeting minutes, insurance policies, files relative to legal matters involving the bank, certain bank employee payroll and personnel files, and all files pertaining to insider loans or suspected fraud. The hardcopy files that Investigations personnel acquire at or after the closing are shipped to the Dallas Regional Office and kept in a locked central file room or maintained in an individual investigator's office. A list of the documents retrieved by Investigations is prepared and placed in the Closing Manager's Book. At the Dallas Regional Office, information from the retrieved documents is loaded into ARMS, and the information in ARMS becomes the inventory for both active and inactive Investigations records. We observed that the investigators' offices were not locked after normal working hours, so anyone having or gaining access to the Dallas Regional Office could gain access to these records.

During one walk-through of the Investigations' area in Dallas, we observed that the file room was unlocked during the day. We also noted that Investigations was not making use of a sign-out sheet. After discussing our observations with the Investigations manager, the manager sent the group an e-mail, which stated "to comply with data

security requirements, the door to the file room needs to be closed and locked when not in use." Subsequently, we visited the location and noted that the file room was locked.

Hardcopy Document Handling and Storage by General Accounting. DRR's General Accounting prepares federal and state tax reporting documents for the receiverships. These reports include Wage and Tax Statements (Forms W-2) to bank employees, Mortgage Interest Statements (Forms 1098) to bank borrowers, and various Forms 1099 that report such information as interest earned and forgiveness of debt. These documents contain a host of personally identifiable information including name, address, SSN, and balances on customer accounts. General Accounting personnel do not remove hardcopy records containing personally identifiable information from the failed financial institutions. Instead, they use the BIS electronic data download to create the aforementioned tax information. General Accounting uses two data systems to create this tax information—Tax Track for receivership tax returns and Checkrite for Forms W-2, 1098, and 1099.

When we began our audit, General Accounting personnel maintained hard copies of Forms W-2, 1098, and 1099 in unlocked file cabinets in two unlocked file rooms. Also, according to one tax accountant, tax files were often left overnight in a person's office until such time as work was completed and the files were placed into the file cabinets. On December 15, 2005, we brought this situation to DRR management's attention and, subsequently, locks were installed on the file room doors, thereby addressing that issue.

Conclusion

DRR was not fully complying with the requirement in FDIC Circular 1210.18, *FDIC Records Management Program,* that each division establish a Records Management Program consistent with FDIC policy. DRR has established certain controls in its Closing Manual and various other procedures and practices to address security for personally identifiable information. However, DRR could better ensure that adequate controls are implemented by establishing a Records Management Program that more broadly defines the types of data that should be secured and the proper means of doing so. Without these additional controls, personally identifiable information is at greater risk of compromise and unauthorized use.

Recommendation

We recommend that the Director, DRR, work with DOA, and other cognizant FDIC divisions and offices, in developing a DRR Records Management Program that includes guidelines for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions.

CORPORATION COMMENTS AND OIG EVALUATION

On September 11, 2006, the Director, DRR, provided a written response to the draft of this report. The DRR response is presented in its entirety in Appendix IV. A summary of management's response to the recommendation is in Appendix V.

In its response, DRR concurred with the recommendation and stated that it is forming a working group, which, in consultation with DOA and others, will develop records management guidance specific to their needs. The guidance will address inventorying, maintaining, using, accounting for, and controlling hardcopy records that contain personally identifiable information.

DRR's planned action is responsive to our recommendation. Accordingly, the recommendation is resolved but will remain open until we have determined the agreed-to corrective action has been completed and is effective.

PRIVACY IMPACT ASSESSMENTS

Based on our review of DRR's inventory of automated systems and discussions with DRR officials, we determined that as of October 2005, DRR had completed PIAs for only 12 of 27 data systems that could have contained personally identifiable information. This shortfall occurred because DRR had completed PIAs only on DRR data systems that DIT had initially identified as containing Taxpayer Identification Numbers (TIN). As a result of this narrow focus, DRR may not have been in full compliance with the E-Government Act of 2002, which we concluded requires that DRR conduct PIAs on all DRR data systems containing bank customer and employee personally identifiable information. Prior to completion of our fieldwork, DRR re-evaluated its systems and conducted PIAs on all those systems warranting the assessments.

In addition to the 12 DRR data systems that DIT had initially identified as containing TIN information, and for which DRR completed PIAs, we identified 15 other DRR systems that appeared to contain personally identifiable information. For example, DRR had not completed a PIA for its Pension Tracking System (PENTRACK), which is used to manage and distribute funds in benefits plans for employees of failed institutions not assumed by an acquirer. A PIA was also not completed for the Best Bank Credit Card System, which is used to administer the credit card portfolio of over 600,000 accounts inherited from Best Bank when it failed. Both of these systems appeared to contain personally identifiable information.

Although DIT initially focused attention on conducting PIAs on FDIC automated systems containing TINs, OMB guidance to agencies on implementing privacy provisions of the E-Government Act suggests that this definition was too narrowly focused. Specifically, OMB guidance states:

> Information in identifiable form is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number 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.)

In late November and early December 2005, we met with DIT and DRR officials to discuss the 15 other DRR data systems that we had identified as possibly containing personally identifiable information. At that time, the officials agreed to reassess the need to complete PIAs on these 15 systems and 3 additional systems that the divisions had independently identified as possibly needing PIAs (thus increasing the total number of systems to 30). As of May 23, 2006, DRR had completed 8 additional PIAs for a total of 20 PIAs related to DRR data systems. DRR notified us that it had determined that the 10 remaining data systems that are assessed do not warrant PIAs because the systems either have been replaced or do not contain personally identifiable information, and we concurred with DRR's assessment.

Because DRR has either completed the required PIAs or determined that PIAs were not warranted for the identified data systems, we are not making a formal recommendation in this report. Additional details on the DRR data systems and PIA status are in Appendix III.

OTHER MATTERS WARRANTING MANAGEMENT ATTENTION

During the course of our audit, we also identified opportunities for the FDIC to improve controls over the protection of personally identifiable information in two other areas. The first area relates to the FDIC's records storage contract with Iron Mountain, and the second to the FDIC's overall Records Management Program.

FDIC's Contract With Iron Mountain

With respect to the FDIC's records management storage contract with Iron Mountain, we found that DOA had not (1) executed a confidentiality agreement with Iron Mountain, (2) developed a contract oversight management plan, and (3) completed background investigations on certain Iron Mountain employees. We addressed these matters and made recommendations in Audit Report No. 06-016 entitled, *Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc*., dated August 10, 2006. As a result, we are not making recommendations in this report regarding the Iron Mountain contract.

FDIC's Records Management Program

We identified opportunities for the FDIC to enhance its overall Records Management Program by more closely complying with existing federal records management guidance promulgated by NARA. Specifically, DOA should consider whether (1) sufficient attention is given in existing policies and procedures to the management of active records, (2) records management training needs to be strengthened, and (3) corporate evaluations of the Records Management Program are adequate.

As previously stated, federal guidance related to records management is promulgated by NARA. NARA guidance specifies that, among other things, agencies must:

- Institute adequate records management controls over the maintenance and use of records wherever they are located to ensure that all records (active and inactive), regardless of format or medium, are organized, classified, and described to promote their accessibility and make them available for use by all appropriate agency personnel for their authorized retention period.

- Ensure that adequate training is provided to all agency personnel on policies, responsibilities, and techniques for the implementation of recordkeeping requirements.

- Evaluate, periodically, agency Records Management Programs relating to records creation and recordkeeping requirements, maintenance and use of records, and records disposition. These evaluations should determine compliance with NARA requirements, including requirements for storage of agency records and storage facilities, and assess the effectiveness of the agency's Records Management Program.

FDIC's Focus on Inactive Records. Circular 1210.18 references the three phases of the life cycle of a record: creation, maintenance, and disposition. However, the circular contains few specific procedures related to the handling of active records. In addition, the FDIC directives on records disposition, records retention and disposition schedules, and standards for creating record inventories focus on the handling of inactive records. Consequently, as a whole, the FDIC's Records Management Program may not adequately consider the handling of active records maintained by FDIC divisions and offices. This impacts DRR because it is responsible for handling failed institution records for which the FDIC, as custodian of those records, has responsibility.

According to DOA's Assistant Director, Corporate Support Section, the FDIC's Records Management Program focuses on inactive records being inventoried and placed into off-site storage. The Assistant Director stated that it is up to the divisions and offices to set policies and procedures for managing records in an active status within their business units.

***FDIC's Records Management Training*.** The FDIC does not provide comprehensive records management training to FDIC employees. Rather, records management training is currently limited to training in the inventorying and retrieving of inactive records using ARMS. Because FDIC personnel are not receiving comprehensive records management training, personnel may not be sufficiently aware of their responsibilities for handling and protecting records containing personally identifiable information.

We discussed the issue of records management training with key DOA and DRR officials. The DOA's Assistant Director, Corporate Support Section, stated that DOA does not provide records management guidance or training to the division records liaisons, although training is available through NARA. DRR Records Liaisons in Washington and Dallas told us that that they have received no formal Records Management Program training. Also, we noted no records management training courses on the Corporate University Web site.

DOA and DRR officials indicated that there is a need for corporate awareness and training on records management procedures and practices. For example, DRR officials stated that the roles of the division Records Liaisons are not well defined, no training other than ARMS usage has been offered, and there is no specific guidance for the Records Liaisons on records management issues. However, DOA is reviewing available NARA training provided by the U.S. Office of Personnel Management and is considering making similar training mandatory for all FDIC employees.

Records Management Program Evaluations. The FDIC has not conducted periodic evaluations of its Records Management Program to determine consistency with NARA regulations. Rather, DOA has conducted only limited evaluations of records handling. For example, in October 2003, DOA conducted an Administrative Compliance Review, which measured compliance with established policies and procedures for records being shipped out of the Dallas Region to Iron Mountain. This review focused on inactive records. In October 2005, DOA performed an Internal Control Review to determine whether records were destroyed in accordance with policy. This review also focused on inactive records.

Additionally, DRR has not assessed division records management practices for compliance with NARA requirements. DRR Records Management Liaisons and Internal Review officials knew of no periodic assessments of records management practices. However, the officials told us that DRR's Senior Management Oversight Committee is completing an initiative to look at records retention and disposition schedules related to inactive records for DRR's various business groups.

Conclusion

The matters discussed above are beyond the scope of this audit. As a result, the OIG has included an audit in its fiscal year 2007 Assignment Plan that will address corporate-wide records management. Accordingly, we are not making recommendations to DOA in this

report. However, we are providing this information for consideration in the drafting of the FDIC records management manual, which is currently ongoing within DOA.

CORPORATION COMMENTS AND OIG EVALUATION

On September 12, 2006, the Director, DOA, provided a written response to the draft of this report. The DOA response is presented in its entirety in Appendix IV. In its response, DOA stated that with respect to the Iron Mountain contract issues, DOA generally agreed with the OIG recommendations made in the OIG report entitled, *Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc.*, and is in the process of taking the necessary corrective actions. With respect to the records management program issues, DOA stated that it has taken steps to establish a control framework in the Records Management Program in order to provide the controls to mitigate potential risks to the FDIC but recognizes that it is important to continue to evaluate and improve upon its business operations. In that regard, DOA indicated that it will consider the information we provided as the division continues to improve the Program.

We consider DOA's comments to be responsive to these two matters. As previously discussed, we will be conducting a future audit in this area and will follow up on DOA's actions at that time.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The overall audit objective was to determine whether DRR adequately protects personally identifiable information collected and maintained as a result of resolution and receivership functions. In this audit, we focused on DRR efforts to protect information maintained in hardcopy form. We limited our review of DRR's protection of sensitive information in electronic form to DRR's completion of risk assessments associated with systems containing such information.

Scope and Methodology

We performed our audit from July 2005 through March 2006 in accordance with generally accepted government auditing standards. We performed field work in DRR, DOA, and DIT offices in Washington, D.C. In addition, we performed field work in the Dallas Regional Office to assess the safeguards over handling and storing failed institutions records currently being maintained by DRR.

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; OMB Circular No. A-130; and Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005.
- Reviewed the DRR Privacy Act System of Record Notices that contained employee information.
- Reviewed and discussed with other OIG audit teams the status of activities and initiatives related to the development of a comprehensive privacy program for the Corporation.
- Reviewed OMB guidance related to conducting PIAs as well as relevant FDIC guidelines. We confirmed that PIAs had been completed on the 20 DRR applications that DRR and DIT determined warranted the assessments.
- Reviewed DRR's resolution and receivership policies, procedures, and practices for safeguarding personally identifiable information during the resolution and receivership process.
- Discussed DRR practices and procedures regarding safeguarding personally identifiable information with each of the DRR operating group managers in the Dallas Regional Office.
- Observed the operations of the Dallas operating group file storage rooms.
- Discussed with DRR Business Project officials in Washington, D.C., DRR initiatives for identifying data systems and safeguarding personally identifiable information within the data systems.

- Obtained NARA information on records management administration guidance and discussed the Records Management Program with the DRR Records Liaisons in the Dallas Regional Office and DRR headquarters.
- Discussed and coordinated our audit with DRR's Internal Review group.

DOA administers a corporate-wide Records Management Program for which we performed the following:

- Reviewed DOA's Records Management Program and pertinent directives.
- Discussed with DOA officials the handling, storage, and retrieval of failed institution records.
- Assessed DOA's storage contract with Iron Mountain and talked with DOA contract oversight officials in Washington, D.C., regarding site visits and contract employee practices relating to safeguarding personally identifiable information.
- Reviewed the FDIC's *Acquisition Policy Manual* to identify provisions related to Contractor Confidentiality Agreements and the Privacy Act and reviewed selected contract files to determine whether appropriate provisions and clauses related to privacy and confidentiality agreements had been included.

Internal Controls

We gained an understanding of relevant control activities by reviewing (1) FDIC security-related directives; (2) DRR policies, procedures, and practices for resolution and receivership functions such as bank closings, asset disposition, claims, and terminations; (3) DRR's initiatives to enhance its privacy program; (4) DIT general rules of behavior for utilizing FDIC information resources; and (5) DOA policies, procedures, and practices for the inventory, handling, storage, and retrieval of inactive failed institution records. We interviewed individuals in DRR, DIT, and DOA involved in protecting and securing personally identifiable information. Based on these reviews, we identified key internal controls over hardcopy documents DRR obtained and generated at institution closings as well as documents DRR was currently maintaining. In the course of our audit, we tested these controls.

Reliance on Computer-Based Data

We did not assess the reliability of computer-based data as it was not significant to meeting our audit objectives.

Compliance With Laws and Regulations, Government Performance and Results Act, and Fraud or Illegal Acts

Regarding compliance with laws and regulations, the Background section of this report discusses various federal laws and guidance related to the protection of personally identifiable information. We considered the FDIC's compliance with these laws and regulations in conducting our audit work. Appendix II lists the specific references to pertinent laws, regulations, and FDIC policies. This report discusses steps that the FDIC

has taken to comply with the intent of these laws and guidance and contains one recommendation for improvement in that regard.

We reviewed the FDIC's performance measures under the FDIC's *Strategic Plan 2005-2010* and the FDIC's 2005 *Annual Performance Plan*. We also reviewed DRR's 2003, 2004, and 2005 Strategic Plans. We determined that neither the FDIC nor DRR have performance measures related to the protection of personally identifiable information.

In consideration of the potential misuse of personally identifiable information for identity theft purposes, we were alert throughout the audit to the potential for fraud and illegal acts. Except for a security breach involving the personal information of current and former FDIC employees, mentioned under the Summary of Prior Coverage below, no instances came to our attention.

Summary of Prior Coverage

The FDIC OIG has issued five prior reports related to safeguarding sensitive information or records storage.

- On August 10, 2006, the OIG issued Audit Report No. 06-016, *Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc.* The objective of the audit was to determine whether the FDIC had adequate controls for ensuring the secure disposal of sensitive information by Iron Mountain. We reported that the FDIC had established a number of key controls to ensure the secure disposal of sensitive information by Iron Mountain. However, we also reported that the FDIC needed to improve its oversight of the Iron Mountain contract to ensure that controls designed to safeguard the disposal of sensitive information were effectively implemented.

- On January 6, 2006, the OIG issued Evaluation Report No. 06-005, *FDIC Safeguards Over Personal Employee Information*. This audit was conducted in response to a security breach involving unauthorized access to personal employee information on a large number of current and former FDIC employees. The objective of the review was to evaluate the FDIC's policies, procedures, and practices for safeguarding personal employee information in hardcopy and electronic form. We reported that the FDIC had a corporate-wide program for protecting personal employee information, had appointed a CPO with responsibility for privacy and data protection policy, and made efforts to enhance its privacy program in response to legislative requirements and breaches of FDIC employee information. We also identified opportunities for the FDIC to strengthen its privacy program for protecting personal employee information.

- On September 16, 2005, 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*, which addressed the status of the FDIC's privacy program and related activities. This audit was conducted in

response to a request for privacy program information contained in OMB's June 13, 2005, memorandum entitled, *FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. The objective of the audit was to determine the current status of the FDIC's efforts to implement a corporate-wide privacy management program. We concluded that although FDIC actions were positive, the FDIC needed to complete a number of ongoing initiatives to ensure adequate protection of personally identifiable employee information in compliance with federal privacy-related statutes, policies, and guidelines.

- On September 30, 2004, the OIG issued Report No. 04-045, *Records Management and Storage*. The objective of this audit was to determine whether (1) the contract for records storage was cost-effective and (2) the FDIC's procedures were consistent with other best practices in the federal government and private industry. We concluded that the FDIC's contract with Iron Mountain, Inc. for records storage could be more cost-effective.

- On February 14, 2003, the OIG issued Report No. 03-012, *Control Over the Use and Protection of Social Security Numbers by Federal Agencies,* on the controls over FDIC use and protection of SSNs. We conducted the review based on congressional interest regarding the widespread sharing of personally identifiable information and occurrences of identity theft. The Chairman, Subcommittee on Social Security, House Ways and Means Committee, asked the President's Council on Integrity and Efficiency (PCIE) to review federal agencies' methods for disseminating and controlling SSN data collected from third parties. The FDIC OIG, as a member of the PCIE, performed the audit to assess the adequacy of the FDIC's control over the use and protection of SSN information. In conducting the audit, we focused on SSN information about non-employees such as depositors, debtors, and loan guarantors that was obtained from failing financial institutions insured by the FDIC. We concluded that third-party access to and use of SSNs and other personally identifiable information was not adequately controlled and monitored.

LAWS, REGULATIONS, AND FDIC DIRECTIVES APPLICABLE TO DRR'S PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Laws, Regulations & Policies	Description
Privacy Act of 1974	Provides specific guidance to federal agencies, including the FDIC, 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 (Federal Information Security Management Act (FISMA))	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 use of internal electronic government processes to improve efficiency and services provided. Section 208 of Title II of the Act, applicable to the FDIC, includes procedures to ensure the privacy of personal information in electronic records, including agency preparation of PIAs on agency information systems. Title III of the Act, or FISMA, contains a number of provisions dealing with the protection of information in agency information systems, as well as other security-related matters. Many of these provisions apply to the FDIC.
Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005	Requires federal agencies, including the FDIC, to designate a Chief Privacy Officer to carry out duties relating to the privacy and protection of personally identifiable information collected and used by federal agencies. The requirements include safeguarding information systems from intrusions, unauthorized disclosures, and disruption or damage.
NARA: Title 36 Code of Federal Regulations, sections 1220.36 et seq.	According to these regulations, promulgated by the NARA, agencies must institute adequate records management controls over the maintenance and use of records wherever they are located to ensure that all records, regardless of format or medium, are organized, classified, and described to promote their accessibility and make them available for use by all appropriate agency staff for their authorized retention period. Agencies must ensure that they maintain adequate information about their records moved to an off-site records storage facility. Agencies must ensure the proper, authorized disposition of their records and must periodically evaluate records management programs. The FDIC follows NARA's regulations as a matter of policy. NARA publishes handbooks, conducts training sessions, and furnishes information and guidance to federal agencies about the creation of records, their maintenance and use, and their disposition.

Laws, Regulations & Policies	Description
OMB Circular No. A-130 *Management of Federal Information Resources*	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, including those of the FDIC, for implementing the reporting and publication requirements of the Privacy Act.
FDIC Circular 6371.1, *Bidders List Preparation and Clearance Process*	Establishes a process for preparing and clearing the bidders list used in resolving failing institutions. DRR will forward only the names of interested bidders to the Division of Supervision and Consumer Protection, which is responsible for pre-approving potential bidders for failing institutions and for assessing the risk to the deposit insurance fund(s) posed by potential resolution transactions.
FDIC Circular 1031.1, *Administration of the Privacy Act*	Updates procedures and provides guidance for the appropriate collection, maintenance, use and/or dissemination of records subject to the Privacy Act of 1974.
FDIC Circular 1210.1, *FDIC Records Retention and Disposition Schedule*	Provides updated guidelines applicable to the maintenance and disposition of records.
FDIC Circular 1210.4, *Records Disposition*	Defines responsibilities for managing the records disposition process and the actions to be taken when records are no longer needed to conduct business.
FDIC Circular 1210.16, *Standards for Creating Records Inventories*	Establishes standards for inventories of failed institution records. The circular distinguishes between inactive and active records, requiring that inactive records be stored off-site.
FDIC Circular 1210.18, *FDIC Records Management Program*	Defines the FDIC's Records Management Program. The circular describes records, recordkeeping, maintenance, use, and disposition procedures. It requires that ARMS be used by divisions and offices to inventory, physically track, and research both corporate and institution records. Use of this system is mandatory for all inactive records stored off-site and for the active asset/credit files of failed institutions.
FDIC Circular, 1301.3, *Data Stewardship Program*	Establish business accountability and responsibility for managing and sharing corporate data.
FDIC Circular 1310.3, *Information Technology Security Risk Management Program*	Updates policies and responsibilities applicable to the FDIC IT Security Risk Management Program.
FDIC Circular 1360.1, *Automated Information Systems (AIS) Security Program*	Assigns roles and responsibilities for ensuring adequate levels of protection for FDIC automated information systems and the information processed, stored, or transmitted by them; and establishes a base program framework for organization-wide IT security program objectives.

Laws, Regulations & Policies	Description
FDIC Circular 1360.8, *Information Security Categorization*	Provides a standard framework for categorizing all information collected or maintained by or on behalf of the FDIC for the purpose of providing appropriate levels of information security according to a range of risk levels.
FDIC Circular 1360.15, *Access Control for Automated Information Systems*	Revises policies and roles and responsibilities for managing access to FDIC automated information systems and data.
DRR Circular 1360.1, *Information Security Responsibilities*	Restates the division's commitment to the protection of information systems against unauthorized access to or modification of information and against the denial of service to authorized users. Also, it restates the division's commitment to safeguarding the Corporation's data and to update security procedures for the division's information systems.
DRR Circular 7010.1, *Request by Debtors of Failed Institutions for Copies of Their Loan Files, Notes, and Other Loan Related Documents*	Advises employees that records should contain only such information about an individual as is relevant and necessary to accomplish a purpose of the agency and the circumstances when information in the system of records may be disclosed to parties other than the debtor.
DRR Circular 7220.5, *Protecting Borrower Identity*	Establishes DRR's policy on the protection of information related to the identity of borrowers and guarantors when offering loans and other debts for sale.

STATUS OF PRIVACY IMPACT ASSESSMENTS FOR DRR DATA SYSTEMS

DRR Data Systems That May Contain Personally Identifiable Information	DRR Data Systems With Completed PIAs (as of 10/31/05)	Additional DRR Data Systems With Completed PIAs (as of 5/31/06)	DRR Data Systems Assessed by DRR and DIT as Not Needing PIAs
Asset Marketing System (AMS)			✓
Asset Reporting Information System (ARIS)			✓
Asset Servicing Technology Enhancement Program (ASTEP)		✓	
Best Bank Credit Card System (BBCC)		✓	
Collateral and Possessory System (CAPS)			✓
Combined Asset Reporting Database (CARD)	✓		
Credit Notation System (CNS)	✓		
Customer Service Contact System (CSCS)			✓
Control Totals Module (CTM)	✓		
Dividend Processing System (DPS)	✓		
DRR Locator and Reporting System (DOLLARS)	✓		
FDIC Automated Corporate Tracking System (FACTS)		✓	
FDIC Real Estate Retrieval System (DRRORE)			✓
FDIC SALES		✓	
FDIC Unclaimed Funds System (FUNDS)		✓	
INTRALINKS			✓
National Asset Inventory System (NAIS)	✓		
National Inventory System (NIS)	✓		
National Insurance System Extranet Web Page (NISExt)	✓		
National Processing System (NPS)			✓
Overarching Automation System (OASIS)	✓		
Owned Real Estate System (ORES)	✓		
Pension Tracking System (PENTRACK)		✓	
PROFORMA (PROFORMA)			✓
Receivership Liability System (RLS)	✓		
Risk Analysis and Value Estimation System (RAVEN*)		✓	
Securitization Transactions Asset and Certification Database (STAC*)			✓
Servicing Request Tracking System II (STSII)	✓		
Subsidiary Information Management Network (SIMAN)			✓
Warranties and Representations Accounts Processing System (WRAPS*)		✓	
Totals 30	**12**	**8**	**10**

Source: OIG analysis of information from the DRR Business Project Manager's Group.

* DRR identified three data systems (RAVEN, STAC, and WRAPS) in addition to the initial 27 data systems the OIG had asked DRR to review. Hence, we have included 30 DRR data systems.

CORPORATION COMMENTS

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Resolutions and Receiverships

DATE: September 7, 2006

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

FROM: Mitchell L. Glassman
Director [Electronically produced version; original signed by Mitchell L. Glassman]
Division of Resolutions and Receiverships

SUBJECT: Response to Draft OIG Audit Report Entitled, *DRR's Protection of Bank Employee and Customer Personally Identifiable Information* (Assignment No. 2005-050)

This memorandum is in response to the recommendation in the Draft Audit Report dated August 11, 2006.

OIG Audit Recommendation:

That the Director, DRR, work with DOA, and other cognizant FDIC divisions and offices, in developing a DRR Records Management Program that includes guidelines for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions.

Response: DRR agrees with the recommendation.

DRR recognizes that, while we have established controls and procedures for the protection of sensitive information contained in failed financial institution records, we can always make improvements in our records management procedures. In fact, we are currently evaluating an electronic labeling and tracking system for potential use to track documents taken into DRR's possession as a result of future financial institution closings. Therefore, we concur with the recommendation contained in the audit results. DRR is forming a working group, which in consultation with DOA and others will develop records management guidance specific to our needs. The guidance will address inventorying, maintaining, using, accounting for, and controlling hardcopy records that contain personally identifiable information. We will issue this guidance by the end of the second quarter 2007.

cc: Arleas Upton Kea, DOA
Daniel H. Bendler, DOA
James H. Angel, Jr., OERM
Ron Bieker, DRR
Gail Patelunas, DRR
James Wigand, DRR
Rick Hoffman, DRR
Steven Trout, DRR

FDIC
Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Administration

DATE: September 12, 2006

MEMORANDUM TO: Stephen M. Beard
Deputy Assistant Inspector General for Audits
[Electronically produced version; original signed by Arleas Upton Kea]

FROM: Arleas Upton Kea, Director
Division of Administration

SUBJECT: DRR's Protection of Bank Employee and Customer Personally Identifiable Information (Assignment Number 2005-050)

The Division of Administration (DOA) has completed its review of the subject Office of Inspector General (OIG) report. We appreciate the review performed by the OIG and its recommendation. The report made one recommendation to the Director, Division of Resolution and Receiverships (DRR), to work with DOA and other FDIC divisions and offices, to develop a DRR Records Management Program (Program). DOA recognizes the need for its involvement in the DRR Program, and will work with DRR in its development. DRR will respond to the report recommendation in a separate memorandum.

Although the report contained one recommendation made to DRR, the OIG did identify opportunities for the FDIC to improve controls in two areas. The first area relates to the FDIC's records storage contract with Iron Mountain, and the second to the FDIC's overall Records Management Program. DOA has evaluated the OIG suggestions and provides the following response.

FDIC's Contract With Iron Mountain.

As stated in the subject report, the OIG found that DOA had not (1) executed a confidentiality agreement with Iron Mountain, (2) developed a contract oversight management plan, and (3) completed background investigations on certain Iron Mountain employees. These matters were brought to the attention of DOA management in the recently issued OIG report entitled *"Controls Over the Disposal of Sensitive FDIC Information by Iron Mountain, Inc."*, dated August 10, 2006. DOA generally agreed with the OIG recommendations made in the August 10 report and has taken or is in the process of taking appropriate corrective actions. The OIG determined that DOA's proposed corrective actions were responsive to the report recommendations.

FDIC's Records Management Program.

DOA has taken steps to establish a control framework in the records management program that provides the controls to mitigate potential risks to the FDIC. At the same time, DOA recognizes that it is important to continue to evaluate and improve upon its business operations. As such, we appreciate the suggestions made by the OIG to enhance the overall Corporate Records

Management Program and will evaluate the various opportunities identified as DOA continues to improve its Program.

If you have any questions regarding the response, our point of contact for this matter is Andrew Nickle, Audit Liaison for the Division of Administration. Mr. Nickle can be reached at (703) 562-2126.

cc: Mitchell L. Glassman, DRR
Steven K. Trout, DRR
Rick Hoffman, DRR
Glen Bjorklund, DOA
Michael Rubino, DOA
Ann Bridges Steely, DOA
James H. Angel, Jr., OERM

2

APPENDIX V

MANAGEMENT RESPONSE TO RECOMMENDATION

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

Corrective Action for the Recommendation: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
DRR is forming a working group, which, in consultation with DOA and others, will develop records management guidance specific to DRR's needs. The guidance will address inventorying, maintaining, using, accounting for, and controlling hardcopy records that contain personally identifiable information.	June 30, 2007	NA	Yes	Open

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

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