Office of Inspector General

September 2008
Report No. AUD-08-015

Protection of Resolution and Receivership Data Managed or Maintained by an FDIC Contractor

Office of Audits

OIG

Office of Audits

Federal Deposit Insurance Corporation

Report No. AUD-08-015 **September 2008**

Protection of Resolution and Receivership Data Managed or Maintained by an FDIC Contractor

Why We Did The Audit

The FDIC's Division of Resolutions and Receiverships (DRR) is responsible for all activities related to the closing, field management, and resolution of failed financial institutions. The objectives of this audit were to (1) determine whether the closing support contract used by the DRR Business Information Systems (BIS) Section contains privacy and information security clauses to protect pre-closing and failed institution data and (2) evaluate the steps the FDIC Oversight Manager (OM) takes to ensure the contractor is complying with privacy and information security clauses.

Background

The FDIC has established a risk-based corporate-wide security program and a privacy program to protect the sensitive information the Corporation manages. These programs include guidance for contractors and OMs to help ensure contractors are complying with government-wide and FDIC information security policies and procedures.

The FDIC collects sensitive information when conducting resolution and receivership activities at FDIC-insured financial institutions. Such information includes personally identifiable information (e.g., name, address, Social Security number, phone number, and account and loan data) for institution depositors, borrowers, and employees. DRR's BIS Section, located in the FDIC's Dallas Regional Office, is responsible for securing all the operating systems, data, and hardware once a failing institution is closed. To that end, DRR has established a Basic Ordering Agreement (BOA) to obtain information technology (IT) support for the BIS Section. A BOA is an agreement setting forth the terms and conditions to be applied to future task orders. The FDIC's policies address the IT security requirements that should be incorporated into IT procurements.

Audit Results

DRR's closing support BOA contains the necessary privacy and information security clauses consistent with FDIC guidance that was in place when the FDIC awarded the contract. Moreover, the Statement of Work contains a clause requiring that the contractor comply with all FDIC policies and procedures, including any new policies and procedures developed during the contract term. For instance, the contractor would be required to comply with the FDIC's policy for safeguarding information described in FDIC Circular 1360.9, *Protecting Sensitive Information*, which became effective after the contract award date.

The OM is taking multiple steps to ensure the contractor is aware of, and complying with, the privacy and information security clauses. For example, the OM reviewed the contractor's IT security plan and routinely monitors the status of background investigations for contractor personnel. The OM is planning to take additional steps to ensure the contractor has complied with the FDIC's training requirements and to sustain contractor attention regarding its responsibilities for safeguarding information. With regard to IT equipment, as necessitated by a business need at the time the FDIC awarded the contract, the FDIC did not furnish the contractor with laptops and has since relied on the contractor to maintain its laptops consistent with FDIC information security standards. In June 2008, DRR established a pool of laptops provided by the Division of Information Technology for contractor use. Furnishing FDIC equipment allows the FDIC to ensure the security of information stored on the laptops and allows contractor personnel to store sensitive data on the laptops as circumstances dictate without violating FDIC policy for protecting sensitive information. With regard to the contractor's laptops used prior to June 2008, the FDIC is requiring that the contractor sanitize those laptops in accordance with FDIC procedures. A Technical Monitor is helping the OM coordinate with the contractor to ensure the process is completed in a timely manner. In the interim, the contractor has physically secured all of its laptops until the sanitization process is completed. The Technical Monitor is maintaining a log to track the deployment of the FDIC's laptops to contractor personnel.

One area warrants additional attention. The Contracting Officer and OM found *Confidentiality Agreements* for only 32 (70 percent) of 46 contractor personnel. *Confidentiality Agreements* document an individual's understanding of, and commitment to, safeguarding data and are a key security requirement under the contract. FDIC policy and the BOA are clear that the Contracting Officer is responsible for ensuring that contractor personnel sign the agreements and for maintaining them in the contract file. Strengthening controls over *Confidentiality Agreements* will help to further protect sensitive resolution and receivership information.

Recommendation and Management Response

We recommended that the FDIC establish controls to ensure that Contracting Officers obtain signed *Confidentiality Agreements* from all contractor personnel required to submit such agreements and maintain copies of those agreements in the contract file. Management concurred with our recommendation and is taking responsive corrective action.

To view the full report, go to www.fdicig.gov/2008reports.asp

Contents

BACKGROUND 2

AUDIT OBJECTIVES 5

AUDIT APPROACH 6

RESULTS OF AUDIT 7

PRIVACY AND INFORMATION SECURITY CLAUSES 9

STEPS TAKEN BY THE OM 15

CONCLUSION 23

RECOMMENDATION 24

CORPORATION COMMENTS AND OIG EVALUATION 25

APPENDICES

1. OBJECTIVES, SCOPE, AND METHODOLOGY 26
2. CORPORATION COMMENTS 31
3. MANAGEMENT RESPONSE TO THE RECOMMENDATION 33
4. ACRONYMS USED IN THE REPORT 34

TABLES

1. OIG Analysis of BIS Closing Support Contract Clauses 11
2. OIG Analysis of Oversight Related to Privacy and Information Security 19

FIGURES

1. Composition of the Contractor's Team 3
2. Summary of the Contractor's Primary Responsibilities 4

Background

- The FDIC's Division of Resolutions and Receiverships (DRR) is responsible for all activities related to the closing, field management, and resolution of failed financial institutions.

- The FDIC has established a risk-based corporate-wide information security program and a privacy program to protect the sensitive information that the Corporation manages. These programs consist of corporate policies, procedures, and guidance; a Chief Information Security Officer and Chief Privacy Officer with overall responsibility for information security and privacy, respectively; Information Security Managers (ISM) within the FDIC's program divisions and offices to ensure a business focus on information security and privacy; and mandatory information security and privacy awareness training for FDIC employees and contractor personnel.

- Key to achieving the FDIC's mission is safeguarding the sensitive information the Corporation collects when conducting resolution activities. Such information includes sensitive personally identifiable information (e.g., names, addresses, Social Security numbers, phone numbers, and account and loan data) for institution depositors, borrowers, and employees.

- Under the umbrella of the corporate program, DRR has established a number of controls to integrate information security and privacy protection into its business operations and systems – including appointing an ISM, defining security business rules for resolution and receivership data, and developing division-specific policies and guidelines for safeguarding the sensitive information the Corporation handles.

Background

- DRR's Business Information Systems (BIS) Section in the Dallas Regional Office is responsible for identifying all electronic equipment, data systems, Web sites, and Internet banking services and products at a failing/failed financial institution and securing all operating systems, data, and hardware once the failing institution is closed.

- In February 2006, DRR established a Basic Ordering Agreement (BOA) with Deloitte Consulting (contractor) to provide information technology (IT) support services required during the resolution of a failed financial institution.

- As the need arises, the FDIC issues a task order, under the terms of the BOA, that details the IT staffing and services required to support a particular failed institution closing. The Contracting Officer (CO) and Oversight Manager (OM) refer to the BOA and the task orders as the BIS closing support contract. Figure 1 illustrates the typical composition of the contractor's team.

Figure 1: Composition of the Contractor's Team

Generally, one or more of the following are on the team:

- IT Manager (Electronic Data Processing Manager)
- IT Security Specialist
- Network Local Area Network (LAN) Specialist (LAN/Wide Area Network Administrator)
- IT Specialist (Hardware Support Specialist)
- IT Specialist (Download Specialist)
- IT Specialist (Data Forensics Specialist) under certain circumstances, as determined by the OM/Technical Monitor (TM)

Source: Statement of Work – BIS closing support contract.

Background

- As of June 19, 2008, the FDIC had awarded 34 task orders under the BOA, which totaled $8.5 million. Figure 2 summarizes the contractor's primary responsibilities.

Figure 2: Summary of the Contractor's Primary Responsibilities

- Coordinate pre-closing plans and activities with the BIS OM/TM, Receiver-in-Charge, and Closing Manager.
- Secure the failed institution's on-site data processing operations, communications systems, e-banking services, Fed Wire, Internet service provider, and networks.
- EDP Manager acts as a point of contact between the closing manager and failed institution's data processing operations staff and its data processing servicer.
- Coordinate processing requirements for all FDIC Closing Team Function Areas.
- Coordinate ongoing operation with the entity purchasing the failed institution.
- Coordinate imaging and storage of documents associated with the failed institution.
- Obtain and deliver data file downloads and reports, as required.
- Map data, convert data, reconcile data to subsidiary trial and general ledger balance totals, and load data to FDIC applications.
- Provide LAN administration and network support for the FDIC's accounting system and the Receivership Liability System LANs.
- Prepare ad hoc reports, letters, and labels, as requested, using mapped downloaded data.
- Provide general hardware and software support to the FDIC Closing Team.
- Preserve and analyze (in certain cases, as defined by the BIS OM/TM) data stored in various electronic media such as desktop personal computers, laptops, network storage devices, palm pilots, personal digital assistants, and cell phones.

Source: Statement of Work – BIS closing support contract.

Audit Objectives

Objective 1 **Privacy and Information Security Contract Clauses**	Determine whether the closing support contract used by DRR's BIS Section contains privacy and information security clauses to protect pre-closing and failed institution data.
Objective 2 **Steps Taken by the OM**	Evaluate the steps the OM takes to ensure the contractor is complying with the privacy and information security clauses in the contract.

Audit Approach

To accomplish our objectives, we:

- Obtained and reviewed contract documents, including the BOA, Statement of Work, and one of the task orders issued for closing support activities.
- Reviewed relevant policies and procedures to identify the contracting requirements and the OM responsibilities with regard to privacy and information security.
- Obtained information from officials in: the Division of Administration (DOA), including the Contracting Officer (CO); DRR, including the OM and officials in DRR's ISM Section; and the Division of Information Technology's (DIT) Information Security and Privacy Staff.
- Consulted with the Counsel to the Office of the Inspector General (OIG) to help us evaluate whether security and privacy clauses were consistent with relevant guidance.

- We conducted this performance audit from April 2008 through June 2008 in accordance with generally accepted government auditing standards. Additional details on our objectives, scope, and methodology are in Appendix 1.

Results of Audit

Privacy and Information Security Clauses in the Closing Support Contract

- DRR's closing support BOA contains the necessary privacy and information security clauses consistent with FDIC guidance that was in place when the FDIC awarded the contract. Moreover, the Statement of Work includes a clause requiring that the contractor comply with all FDIC policies and procedures, including any new policies and procedures developed during the contract term. For instance, the contractor would be required to comply with the FDIC's guidance for safeguarding information described in FDIC Circular 1360.9, *Protecting Sensitive Information*, which became effective after the contract award date.

Steps Taken by the OM to Ensure Compliance with the Privacy and Information Security Clauses

- The OM is taking multiple steps to ensure the contractor is aware of, and complying with, the privacy and information security clauses. For example, the OM reviewed the contractor's IT security plan and routinely monitors the status of background investigations for contractor personnel. Further, the OM is planning to take additional steps to ensure the contractor has complied with the FDIC's training requirements and to sustain contractor attention regarding its responsibilities for safeguarding information.

Results of Audit

- With regard to IT equipment, as necessitated by a business need at the time the FDIC awarded the BOA, the FDIC did not furnish the contractor with laptops. Therefore, the FDIC relied on the contractor to maintain security features on its laptops consistent with FDIC policies; however, use of the contractor's laptops created a potential risk related to sensitive FDIC data. In June 2008, DRR established a pool of 25 laptop computers supplied by DIT for the contractor's use to ensure that any sensitive data collected during the resolution process is stored only on FDIC IT equipment. All laptops in the pool are fully encrypted to protect data if the equipment is lost or stolen. Furnishing FDIC equipment allows the FDIC to ensure the security of its laptops and allows contractor personnel to store sensitive data on the laptops as circumstances dictate without violating the FDIC's policy, established in 2007, for protecting sensitive information.

- With regard to the contractor's laptops used during the resolution process (prior to 2008), the FDIC is requiring the contractor to sanitize those laptops and to provide a certification to the FDIC that this critical step was done in accordance with FDIC standards. The contractor has physically secured all those laptops until the sanitization process is completed. A TM is helping the OM to coordinate with the contractor to ensure the sanitization is done in a timely manner. DRR is responsible for tracking, cleaning, and reissuing the pool of laptops.

- We found one area that warrants management attention. The CO and OM found *Confidentiality Agreements* for only 32 (70 percent) of 46 contractor personnel. *Confidentiality Agreements* document an individual's understanding of, and commitment to, safeguarding data and are a key security requirement under the closing support contract. Although the CO and OM were certain that all the agreements had been signed by contractor personnel, neither one had ensured the agreements were maintained in the contract file. As such, we could not verify that agreements had been obtained as required. We are making a recommendation to DOA to establish controls to help ensure that contractor personnel complete and submit the agreements as required and that the CO maintains copies of all agreements in the contract file.

Privacy and Information Security Clauses

FDIC Guidance for Privacy and Information Security Clauses

- The *Acquisition Policy Manual* (APM) and Interim Acquisition Policy Memorandum 2003-2, *Implementing IT Security in FDIC Procurements*, dated November 7, 2003, establish the FDIC policies and procedures for incorporating IT security requirements into IT procurements. Additionally, the FDIC revised the standard contracting documents to ensure that IT security requirements were fully addressed in all phases of the IT procurement lifecycle when Memorandum 2003-2 was issued.

- The APM and Interim Acquisition Policy Memorandum referenced the following Circulars:

  - FDIC Circular 1610.2, *Security Policy and Procedures for FDIC Contractors and Subcontractors*, dated August 1, 2003, establishes the security policy and procedures that must be followed for contractors and subcontractors to do business with the FDIC.

  - FDIC Circular 1360.17, *IT Security Guidance for FDIC Procurements/Third Party Products*, dated June 30, 2003, provides guidance regarding the consideration of security in contract planning, incorporation of security requirements in the contract, and the oversight of contractor information security practices.

Privacy and Information Security Clauses

Privacy and Information Security Clauses in the Closing Support Contract

- DRR worked with DOA to establish IT procurement requirements relevant at the time the closing support BOA was awarded. Since the award of the BOA, the FDIC's privacy and information security program has continued to evolve. For example, the FDIC issued Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, which establishes FDIC policy on protecting sensitive information collected and maintained by the Corporation and guidance for safeguarding the information.

- The standard contract documents (i.e., BOA, Statement of Work, task order) have been updated to more specifically address the FDIC's current privacy and information security policies. Further, DOA, DIT, and the Legal Division are currently updating a number of standard clauses to coincide with the new acquisition policy being drafted.

- The FDIC's privacy and information security program has continued to evolve, and the closing support contract documents (i.e., the BOA and Statement of Work) require that the contractor comply with all FDIC policies and procedures, including new policies and procedures developed during the term of the contract.

- Table 1 on the next page identifies the FDIC's key IT procurement requirements and summarizes the clauses contained in the BIS closing support contract that are in place to address the requirements.

Privacy and Information Security Clauses

Table 1: OIG Analysis of BIS Closing Support Contract Clauses

Key IT Procurement Requirements	Corresponding Clause in BIS Closing Support Contract
Return or Destruction of Hardcopy and Electronic FDIC Data	☑ **1.2 *Duties*** - The contractor must ensure that all connections and access to the FDIC network and systems are removed and no longer active when the contract expires, and the contractor is subject to pre-exit clearance procedures. ☑ **3.5.1 *Compliance Requirements*** - references the FDIC's policy related to hardcopy and electronic data destruction (Circular 1360.17, *IT Security Guidance for FDIC Procurement/Third Party Products*, dated June 30, 2007).
Risk-level Designation	☑ **3.2 *Risk Level Designation*** - This contract has a high-risk designation. The post-award background investigations and fingerprinting required for all contractor employees will be for this risk level.

Privacy and Information Security Clauses

Table 1: OIG Analysis of BIS Closing Support Contract Clauses (Continued)

Key IT Procurement Requirements	Corresponding Clause in BIS Closing Support Contract
Contractor Confidentiality Agreements	☑ **3.3** ***Confidentiality of Information, Data, and Systems*** - Contractor must ensure the confidentiality of all information, data, and systems provided by the FDIC or used or obtained by contractor personnel under this contract and prevent inappropriate or unauthorized use or disclosure. Contractor personnel must sign *Confidentiality Agreements*.
Personnel Suitability Requirements	☑ **3.1** ***Background Investigations*** - Contractor personnel are subject to background investigations. In addition, contractor personnel performing work on-site must submit to a fingerprint and credit check before receiving on-site identification and access control badges.

Privacy and Information Security Clauses

Table 1: OIG Analysis of BIS Closing Support Contract Clauses (Continued)

Key IT Procurement Requirements	Corresponding Clause in BIS Closing Support Contract
Reference to FDIC Security Policies, Procedures, Laws, and Regulations	☑ **1.4 *Standard of Performance*** - The contractor must at all times comply with FDIC policies, procedures, and directives. ☑ **3.5.1 *Compliance Requirements*** - The contractor's IT Security Plan must be compliant with the identified federal laws and policies and procedures. ☑ **12.2 *Privacy Act*** - Establishes requirements to ensure Privacy Act compliance whenever the contractor is required to design, develop, or operate a system of records on individuals to accomplish an FDIC function.
Security Plan	☑ **3.5 *IT Security Plan*** - The contractor must implement and maintain an IT Security Plan that is compliant with federal laws and FDIC policies and procedures.

Privacy and Information Security Clauses

Table 1: OIG Analysis of BIS Closing Support Contract Clauses (Continued)

Key IT Procurement Requirements	Corresponding Clause in BIS Closing Support Contract
Mandatory Information Security Training	☑ **3.6** ***Training Requirements*** - The contractor must ensure that its personnel receive training at least annually in IT security awareness and security practices. ☑ **3.7** ***Security Awareness Website Training*** - The contractor must review the FDIC's Security Awareness Website.
Network Access	☑ **3.8.1** ***Network Access Requirements*** - The contractor must comply with all provisions of Circular 1360.17, *IT Security Guidance for FDIC IT Procurement/Third Party Products*.

Source: OIG Analysis of APM, FDIC policies, and BIS closing support contract documents.

Steps Taken by the OM

FDIC Guidance for OMs Related to Privacy and Information Security

- Various FDIC policies and procedures describe the OM's responsibilities for overseeing the contractor's compliance with privacy and information security clauses. Key guidance is contained in the following:
  - The FDIC's APM and interim guidance establish policies and procedures for procuring goods and services, identify roles and responsibilities for all FDIC employees involved in the procurement process, and include specific guidance related to IT security in FDIC procurements.
  - FDIC Circular 1360.17, *IT Security Guidance for FDIC Procurements/Third Party Products*, dated June 30, 2003, specifically addresses the OM's role and responsibilities with respect to the oversight of contractor information security practices.
  - FDIC Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007, establishes policy on protecting sensitive information collected and maintained by the Corporation and provides guidance for safeguarding the information. This circular describes the OM's responsibilities with respect to the policy.

Steps Taken by the OM

OIG Evaluation of Steps Taken by the OM

- We found that the OM for the BIS closing support contract is taking multiple steps to ensure the contractor is aware of, and complying with, the privacy and information security clauses. Additionally, to ensure compliance with FDIC training requirements and sustain focus on the contractor's responsibility for safeguarding FDIC data, the OM is planning to:
  - Verify that contractor personnel have completed required information security and privacy awareness training before they work on closing support assignments. We believe this step, coupled with DRR's routine tracking of completed training, will provide the OM with additional assurance that the contractor is complying with this provision of the contract and FDIC policy.
  - Meet quarterly with all contractor personnel to reinforce the FDIC's IT privacy and information security requirements. These meetings will serve as a useful reminder of the FDIC's policies and procedures for protecting data.

Steps Taken by the OM

- Furthermore, with regard to IT equipment, the FDIC did not furnish the contractor with laptops as necessitated by a business need at the time the FDIC awarded the contract in 2006. Therefore, the FDIC relied on the contractor to maintain security features on its laptops consistent with FDIC information security standards. In June 2008, DRR established a pool of 25 laptops for the contractor's use. The laptops were provided by DIT, and all DRR BIS pool laptops are fully encrypted to protect the data if the equipment is lost or stolen. Furnishing FDIC equipment allows the FDIC to ensure the security of information stored on the laptops and allows contractor personnel to store sensitive data on the laptops as circumstances dictate without violating the FDIC's policy for protecting sensitive information. The FDIC's Circular 1360.9, *Protecting Sensitive Information*, states that storage of sensitive electronic information is allowed only on corporate IT equipment. DRR's BIS is responsible for tracking, cleaning, and reissuing the pool of laptops.

- With regard to the contractor's laptops used from the inception of the contract until June 2008, the FDIC has required the contractor to sanitize (remove sensitive information) those laptops and to certify that it is using FDIC sanitization procedures. The contractor has physically secured all of those laptops until the sanitization process is completed. A TM is (1) helping the OM coordinate with the contractor to ensure that sanitization is done in a timely manner and (2) maintaining a log to track the deployment of FDIC laptops to contractor personnel.

Steps Taken by the OM

- We found one area that warrants attention by the CO and the OM. The CO and the OM found signed *Confidentiality Agreements* for only 32 (70 percent) of 46 contract employees. *Confidentiality Agreements* are a requirement, under the terms of the BOA, used to establish a mutual agreement between the FDIC and the contractor employee on the appropriate use and disclosure of confidential information. Various FDIC policies, including Circulars 3700.16, 1360.17, 1360.1, and 1360.9 detail the OM's responsibilities for ensuring that the contractor is complying with the terms of a contract. Additionally, the FDIC APM and interim APM guidance state that contractor personnel must sign and return the *Confidentiality Agreements* to the CO and that the CO is responsible for ensuring signed agreements are retained in the contract file. The BOA is also clear on the need for contractor employees to return signed *Confidentiality Agreements* to the CO.

- The CO and the OM are certain that all 46 contractor personnel signed the agreements, but the OM stated that some contractor personnel had inadvertently submitted the agreements to the Dallas Regional Office security staff along with background investigation paperwork. The OM is working with the CO to obtain copies of the agreements that are missing from the contract file.

- Table 2 on the next page summarizes OM responsibilities and describes the steps being taken and planned by the OM to oversee the contractor's compliance with privacy and information security requirements.

Steps Taken by the OM

Table 2: OIG Analysis of Oversight Related to Privacy and Information Security

OM's Oversight Responsibility	Steps Taken	Ongoing Oversight Planned
Information Security Roles and Responsibilities	☑ The OM stated that the terms of the contract were reviewed at the post-award conference with specific attention given to information security. ☑ Additionally, the OM and TMs provide contractor personnel with BIS-specific training that includes a module on data protection and adherence to all relevant IT directives.	☑ The OM stated that beginning in July 2008, a quarterly meeting will be held with all contractor personnel to, among other things, reinforce the need to comply with FDIC privacy and information security program requirements.
Background Investigations	☑ The OM works with the CO to ensure that contractor personnel submit a fingerprint application and credit report authorization to DOA's Security Management Section. Contractor employees are not permitted to begin working on-site unless a favorable fingerprint records check and credit report are received. The OM tracks approvals received from DOA's Security Management Section and coordinates with the CO and Security Management Section to ensure that contractor personnel have submitted the paperwork necessary for a high-risk position.	☑ The OM will continue to ensure that new contractor personnel comply with this requirement.

Steps Taken by the OM

Table 2: OIG Analysis of Oversight Related to Privacy and Information Security (Continued)

OM's Oversight Responsibility	Steps Taken	Ongoing Oversight Planned
IT Security Plan	☑ The OM reviewed and approved the IT Security Plan submitted by the contractor. ☑ The OM also submitted the IT Security Plan to DRR's ISM for review and approval.	☑ The OM will continue to monitor compliance with the IT Security Plan through ongoing oversight of the contractor's performance.
Training	☑ The OM maintains a list to track whether contractor personnel have received required training. The training information is obtained from DRR's ISM. However, this list was not up to date at the time of our review, and a TM followed up with the ISM to verify that all contractor personnel had received appropriate training.	☑ Going forward, the OM plans to verify that contractor personnel have completed required IT information security and privacy awareness training before they work on tasks that involve sensitive data. The OM and DRR's ISM determined that this step, coupled with routine tracking of training, would provide additional assurance that the contractor personnel met critical training requirements.

Steps Taken by the OM

Table 2: OIG Analysis of Oversight Related to Privacy and Information Security (Continued)

OM's Oversight Responsibility	Steps Taken	Ongoing Oversight Planned
Site Visits and/or Performance Evaluations	☑ The OM, in conjunction with designated TMs, monitors the contractor's work on-site at Dallas or at the site of resolution activity. Unresolved performance issues are brought to the attention of the CO. ☑ The CO, TMs, and OM meet biweekly with key contractor personnel and FDIC subject matter experts to discuss performance or other contract issues.	☑ The OM and TMs will continue to monitor the contractor's compliance with the privacy and information security provisions through ongoing oversight of the contractor's performance. Any issues specific to privacy or information security will be discussed at the biweekly contract status meetings as needed.
Secure Network Equipment	☑ Until June 2008, contractor personnel used their own stand-alone laptops. The OM stated the contractor's laptops were equipped with necessary security and encryption tools in order to protect data. The OM also stated that FDIC data was not stored on contractor equipment unless contractor personnel were in a "travel mode." ☑ FDIC desktops are available in a secure room for contractor personnel use to upload data to FDIC systems.	☑ DRR has a pool of 25 FDIC laptops supplied by DIT for the BIS closing support contract work in lieu of relying on the contractor to maintain its laptops consistent with FDIC security requirements. All DRR BIS pool laptops are fully encrypted to protect the data if the equipment is lost or stolen. ☑ DRR is responsible for tracking, cleaning, and reissuing the laptops in the pool. A TM is maintaining a log to track the deployment of the laptops to contractor personnel. ☑ With regard to the contractor's laptops used prior to June 2008, the contractor is currently sanitizing its laptops and must provide a certification to the FDIC that this critical step was completed in accordance with FDIC standards. The OM and a TM are coordinating with the contractor to ensure this process is completed in a timely manner.

Steps Taken by the OM

Table 2: OIG Analysis of Oversight Related to Privacy and Information Security (Continued)

OM's Oversight Responsibility	Steps Taken	Ongoing Oversight Planned
Confidentiality Agreements	☑ The OM stated that contractor employees were submitting the *Confidentiality Agreements* along with their background investigation forms to the Dallas Security Section. However, the *Confidentiality Agreements* should have been submitted to the CO and placed in the contract file. ☑ Because this was not done, the CO and OM found copies of agreements for only 32 of the 46 contractor personnel working on this contract. We could not, therefore, verify that all contractor personnel working on this contract had, in fact, executed *Confidentiality Agreements*.	☑ The CO is responsible for obtaining the *Confidentiality Agreements* for the contractor personnel. Currently, the OM is working with the CO to obtain copies of all the *Confidentiality Agreements* from the contractor personnel. Going forward, the OM plans to work closely with the CO to ensure that *Confidentiality Agreements* for new contractor personnel are included in the contract file. We made a recommendation to DOA to strengthen controls in this area.

Source: OIG Analysis of FDIC policies and discussions with CO, OM, and TM.

Conclusion

- DRR's closing support BOA contains the necessary privacy and information security clauses consistent with FDIC guidance that was in place when the FDIC awarded the BOA. The OM plays a key role in ensuring that the contractor complies with the FDIC's security requirements in order to help ensure that sensitive information is protected. As Table 2 indicates, we found that the steps being taken by the OM for the BIS closing support contract aligned with established OM responsibilities. In addition, the OM is planning to take steps to ensure the contractor has complied with the FDIC's training requirements and to sustain contractor attention on its responsibilities for safeguarding information, including:

  - Working with the ISM to verify that all contractor personnel have completed required privacy and IT security awareness training. In addition to routine tracking that occurs, the OM and ISM determined they will also begin verifying that contractor personnel have complied with annual training requirements before individual contractor employees are assigned to closing support tasks.

  - Ensuring the contractor completes the sanitization process and provides the FDIC with the necessary certification.

  - Keeping an up-to-date accurate log of FDIC-furnished equipment to minimize the risk to sensitive corporate data.

Recommendation

- We recommend that the Director, DOA:
  - Develop a control mechanism to ensure that COs obtain signed *Confidentiality Agreements* from all contractor personnel required to submit such agreements and that copies of those agreements are maintained in the contract file.

Corporation Comments and OIG Evaluation

- On August 28, 2008, the Director, DOA, provided a written response to the draft of this report. Management's response is presented in its entirety in Appendix 2. Management concurred with our finding and recommendation.

- In response to the recommendation, DOA's Acquisition Services Branch will include *Confidentiality Agreements* in the *Contracts Internal Review Checklist*, currently under development, to ensure that *Confidentiality Agreements* are provided by the contractor and that the CO has uploaded these agreements into the contract file at the time of contract award and whenever changes occur in personnel required to submit the agreements.

- A summary of management's response to the recommendation is in Appendix 3. DOA's planned actions are responsive to our recommendation. The recommendation is resolved but will remain open until we determine that the agreed-to corrective actions have been completed and are responsive.

OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

The objectives of this audit were to (1) determine whether the closing support contract used by DRR's BIS Section contains privacy and information security clauses to protect pre-closing and failed institution data and (2) evaluate the steps the OM takes to ensure the contractor is complying with the privacy and information security clauses.

We conducted this performance audit from April 2008 through June 2008 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope and Methodology

The scope of this assignment focused on privacy and information security clauses in the BIS closing support contract (BOA-FDIC1-050) and one task order (Task Order 2007-006), awarded under the BOA. We reviewed these documents to determine if the privacy and security clauses are in compliance with FDIC policies. We selected this task order because it accounted for approximately 43 percent of the total amount awarded as of June 19, 2008.[1] For purposes of evaluating the steps taken by the OM to monitor compliance with the contract clauses related to security and privacy awareness training, background investigations, and *Confidentiality Agreements*, we took into consideration all 46 of the contractor personnel the OM and CO identified as working on the task order under the BOA.

Evaluation of the Privacy and Security Clauses

To achieve our objectives, we:

- Obtained and reviewed various contract-related documents, including the BOA, Task Order 2007-006, the Statement of Work, and the contractor's IT Security Plan.

- Obtained information from officials in DOA's Acquisition Services Branch and DIT's Information Security and Privacy Staff to gain an understanding of privacy and information security clause guidance that existed when the BOA was awarded in 2006 as well as to gain an understanding of evolving requirements. We also interviewed officials in DRR, including the OM and a TM, and representatives from DRR's Information Security Unit.

[1] The contract total as of June 19, 2008 was $8,475,611. The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

- Reviewed the FDIC's policies and procedures, including:
    - The FDIC's APM and Interim Acquisition Policy Memorandum 2003.2, *Implementing IT Security in FDIC Procurement*s.
    - Circular 1360.1, *DRR Information Security Responsibilities*, dated November 18, 2005.
    - Circular 1360.16, *Mandatory Information Security Awareness Training*, dated July 23, 2002.
    - Circular 1360.17, *IT Security Guidance for FDIC Procurement/Third Party Products*, dated June 30, 2003.
    - Circular 1360.9, *Protecting Sensitive Information*, dated April 30, 2007.
    - Circular 1610.2, *Security Policy and Procedures for FDIC Contractors and Subcontractors*, dated August 1, 2003.
    - Circular 3700.16, *DRR Contract Management*, dated January 17, 2008.
    - DRR's *Guidelines for Protecting Sensitive Information*.
- Consulted with the Counsel to the OIG to evaluate the privacy and information security contract clauses.

Internal Control

We assessed key FDIC internal controls related to privacy and security clauses, including:

- Relevant FDIC and DRR policies, procedures, guidance, and training.
- The roles and responsibilities of the OM and TMs.

Additionally, we selected a random sample of contractor personnel and verified that DOA's Security Management Section had completed required background investigations for the sampled contractor personnel commensurate with the high-risk designation for this contract. We noted no exceptions.

Reliance on Computer-processed Information

Our audit objective did not require that we assess the reliability of computer-processed information, and we did not rely on computer-processed information to support our significant findings, conclusions, and recommendations. Our assessment centered on reviewing hardcopy contract documentation provided by the CO and OM.

Performance Measurement

We reviewed the FDIC's *2005-2010 Strategic Plan* and *2008 Annual Performance Plan* to identify and understand the FDIC's goals, objectives, and ongoing initiatives related to privacy and information security. The FDIC's *2008 Annual Performance Plan* provides an overview of planned 2008 initiatives to enhance the Corporation's management of its key strategic resources. Initiatives address IT Resource Management, the Corporate Privacy Program, and Information Security Program.

DIT has issued a *Privacy Program Strategic Framework* that establishes a formal, comprehensive strategic framework that integrates the FDIC's privacy program mission, vision, principles, goals and objectives, governance structure, key initiatives and activities, performance measurement, monitoring and methods for reporting, and roles and responsibilities.

Compliance With Laws and Regulations

The following laws and regulations were relevant to our objectives.

- Privacy Act of 1974;
- Gramm-Leach Bliley Act;
- Section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act 2005;
- FDIC's Rules and Regulations – Parts 309, *Disclosure of Information;* and 310, *Privacy Act Regulations*; and
- 12 Code of Federal Regulations Part 366, *Minimum Standard of Integrity and Fitness for an FDIC Contractor.*

We found no instances where the FDIC was not in compliance with applicable laws and regulations.

We assessed the risk of fraud and abuse related to the audit objective in the course of evaluating audit evidence.

Prior Coverage

We considered the following reports issued by the FDIC OIG in planning and conducting our work:

- Audit Report No. 07-013 entitled, *Response to Privacy Program Information Request in OMB's Fiscal Year 2007 Reporting Instructions for FISMA and Agency Privacy Management*, dated September 2007. The objective of the audit was to assess the status of the FDIC's privacy program activities and initiatives. The reported concluded that the FDIC continues to take action to safeguard its personally identifiable information (PII) and related systems and address privacy-related provisions of recent Office of Management and Budget memoranda. Of particular note, the FDIC has provided privacy-awareness training. The report contained no recommendations.

- Audit Report No. 07-010 entitled, *Division of Resolutions and Receiverships Protection of Electronic Records*, dated September 2007. The objective of the audit was to evaluate the design and implementation of selected controls established by DRR for safeguarding sensitive electronic information collected and maintained as a result of resolution and receivership activities at FDIC-insured institutions. DRR has established a number of important controls to safeguard the sensitive electronic information it collects and maintains as a result of resolution and receivership activities at FDIC-insured financial institutions. However, a number of deficiencies were identified that increased the risk of unauthorized use of sensitive information. DRR and DIT security officials took prompt action to restrict access to vulnerable sensitive information that we identified during the audit and agreed to the four recommendations made in the report to strengthen controls.

- Evaluation Report No. EM-07-004 entitled, *Risk Designation Levels for Information Technology Staff and Privacy Act Clauses in FDIC Contracts*, dated August 2007. The objective of the evaluation was to identify best practices at other federal agencies pertaining to risk designation levels for IT agency staff and Privacy Act clauses in FDIC contracts. With regard to the contract clauses, the report states that the Privacy Act clause currently incorporated in FDIC contracts was consistent with federal contracting requirements.

- Audit Report No. 06-017 entitled, *DRR's Protection of Bank Employee and Customer Personally Identifiable Information*, dated September 2006. The objective of this audit was to determine whether DRR adequately protects PII collected and maintained as a result of resolution and receivership functions. The audit focused attention on DRR efforts to protect PII in hardcopy form. DRR has established certain controls over the resolution and receivership process, addressing the protection of sensitive bank employee and customer PII. However, given the increased risks associated with, and attention being placed on, identity theft, the audit identified opportunities for DRR to strengthen controls over its

handling of sensitive bank employee and customer PII 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. The report recommended that DRR work with DOA, and other cognizant FDIC divisions and offices, in developing a DRR Records Management Program. DRR agreed with the recommendation.

- Audit Report No. 03-043, *Follow-up Audit of Information Security Management of FDIC Contractors*, dated September 2003. The objective of this audit was to determine whether the FDIC had made adequate progress in addressing recommendations in Audit Report No. 02-035 entitled, *Information Security Management of FDIC Contractors*, dated September 2002. The audit focused on information security in acquisition planning, contract security provisions, and contractor oversight. The report concluded that the FDIC had developed and was finalizing policies and procedures to address the prior audit report's recommendations regarding security in acquisition planning, contract requirements, and contractor oversight. The report included a recommendation for the FDIC to update its *Policy on Off-site Contractor Network Connectivity*. The FDIC agreed to the recommendation.

CORPORATION COMMENTS

FDIC

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226-3500

August 28, 2008

MEMORANDUM TO: Russell A. Rau
Assistant Inspector General for Audits

FROM: Arleas Upton Kea
Director, Division of Administration

SUBJECT: Management Response to the Draft OIG Audit Report Entitled, *Protection of Resolution and Receivership Data managed or Maintained by an FDIC Contractor (Assignment No. 2008-028)*

This is in response to the subject Draft Office of Inspector General (OIG) Audit Report, issued July 29, 2008. In its report, the OIG made one recommendation to the Division of Administration.

We appreciate the review the OIG has performed and recognize that additional steps could be taken to enhance the controls in place regarding the maintaining of Contractor Confidentiality Agreements. This response outlines our planned corrective action for the one recommendation cited in the OIG's Report.

MANAGEMENT DECISION

Finding: Maintain Contractor Confidentiality Agreements in the Contract File

Recommendation 1: That the Director, Division of Administration (DOA) develop a control mechanism to ensure that COs obtain signed Confidentiality Agreements from all contractor personnel required to submit such agreements and that copies of those agreements are maintained in the contract file.

Management Response 1: DOA concurs with the recommendation.

Corrective Action: The policy and procedures for obtaining Confidentiality Agreements from contractors changed with the implementation of the new Acquisition Policy Manual (APM) and its supplemental Procedures, Guidance and Information (PGI) document on August 22, 2008 (see attached). Sections 5.104(b) of the revised APM and PGI require that a Confidentiality Agreement be obtained from an authorized representative of the contractor and from all key personnel prior to receiving or collecting sensitive information. Under the revised policy, non-key personnel are no longer required to sign a Confidentiality Agreement as they are covered under the Contractor's agreement. In all cases, it is the responsibility of the Contracting Officer (CO) to ensure that copies are obtained, and filed in the official contract file (CEFile). Any changes in key personnel require the CO to issue a modification to the contract and key personnel may not work under the contract until they have provided a Confidentiality Agreement to the CO. Additionally, the Acquisition Services Branch will include this item in the Contracts

* The attachment is not included in this appendix but can be provided under separate cover.

Internal Review Checklist, currently under development, to ensure that Confidentiality Agreements are provided by the contractor and key personnel at time of contract award and whenever changes in key personnel occur, and that the CO has uploaded these agreements into CEFile. The Contracts Internal Review Checklist will be completed by December 31, 2008.

Completion Date: December 31, 2008.

If you have any questions regarding this response, the point of contact for DOA is William Gately at (703) 562-2118.

cc: Glen Bjorklund, DOA
Michael J. Rubino, DOA
Elizabeth Walker, DOA
James H. Angel, Jr., OERM
William J. Gately, Jr., DOA

2

MANAGEMENT RESPONSE TO THE 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: Taken or Planned for the Recommendation	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
DOA's Acquisition Services Branch will include *Confidentiality Agreements* in the *Contracts Internal Review Checklist*, currently under development, to ensure that *Confidentiality Agreements* are provided by the contractor and that the CO has uploaded these agreements into the contract file.	December 31, 2008	$0	Yes	Open

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

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

ACRONYMS USED IN THE REPORT

APM	Acquisition Policy Manual
BIS	Business Information Systems
BOA	Basic Ordering Agreement
CO	Contracting Officer
DIT	Division of Information Technology
DOA	Division of Administration
DRR	Division of Resolutions and Receiverships
EDP	Electronic Data Processing
ISM	Information Security Manager
IT	Information Technology
LAN	Local Area Network
OM	Oversight Manager
PII	Personally Identifiable Information
TM	Technical Monitor