Office of Inspector General

November 2007
Report No. AUD-08-002

Examination Procedures for Assessing Selected Controls Related to the Protection of Customer and Consumer Information at Multi-regional Data Processing Servicers (MDPS)

AUDIT REPORT

Office of Audits

oig

Office of Audits

Background and Purpose of Audit

FDIC-insured financial institutions are increasingly outsourcing their critical information technology services to Technology Service Providers (TSP). Frequently, these outsourcing arrangements involve the collection, processing, and storage of customer and consumer information on behalf of financial institutions. The Bank Service Company Act provides federal bank regulators with examination access to TSPs. TSPs that process mission-critical applications for a large number of financial institutions with multiple regulators or geographically dispersed data centers are subject to interagency examination under the Federal Financial Institutions Examination Council's (FFIEC) MDPS program and related examination guidance.

Federal regulators published interagency guidelines that established information security standards for financial institution use in developing and implementing safeguards to protect customer and consumer information. Those guidelines implement statutory requirements for financial institutions intended to protect such information and to deter identity theft. Our audit focused on three selected security control areas contained in the guidelines: the oversight of TSP third-party service providers, incident response programs, and the disposal of information.

The audit objective was to assess the FDIC's implementation of FFIEC and FDIC examination guidance for selected controls related to the protection of customer and consumer information at TSPs in the MDPS program. Of the 16 TSPs in the MDPS program, we sampled 3 of the 8 TSPs for which the FDIC served as the Agency-in-Charge for the most recent examination.

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

Report No. AUD-08-002
November 2007

Examination Procedures for Assessing Selected Controls Related to the Protection of Customer and Consumer Information at Multi-regional Data Processing Servicers (MDPS)

Results of Audit

The FDIC has taken a number of proactive steps in its oversight of TSPs in the MDPS program. During our audit, the FDIC hosted the *2007 FFIEC MDPS Supervisory Strategy Meeting*, enhanced its monitoring of TSPs in the MDPS program, and conducted a number of outreach initiatives. Importantly, FDIC examiners use FFIEC and FDIC examination guidance when assessing security controls related to the protection of customer and consumer information at TSPs in the MDPS program. Additionally, as part of each examination, the examiners considered the risk assessment of security controls prepared by the TSP in response to the interagency guidelines. However, the risk assessments for the three TSPs we reviewed generally did not address the three security control areas (oversight of TSP third-party service providers, incident response programs, and the disposal of information) covered by our audit, and examination documentation we reviewed generally did not contain conclusions on security risks in these control areas. As a result, we were unable to determine whether related examination procedures performed at the three TSPs reviewed were commensurate with the risk of unauthorized access to customer and consumer information.

The FDIC can further ensure that TSP examination procedures are effective and efficient by more closely linking examination procedures to underlying conclusions on risk in security control areas. In this manner, the FDIC would have greater assurance that customer and consumer information processed by TSPs in the MDPS program is protected consistent with statutory and regulatory requirements.

Recommendations and Management Response

We recommended that the Director, Division of Supervision and Consumer Protection: (1) provide conclusions on the risks for key security control areas in FDIC examination documentation for examinations of TSPs in the MDPS program in order to provide greater assurance that examination procedures performed are commensurate with identified risks and (2) conduct periodic quality assurance reviews of examination documentation prepared by FDIC examiners under the MDPS program to achieve greater assurance that MDPS examination documentation contains risk determinations for key security control areas, procedures performed are commensurate with identified risk, and examination processes are consistently applied across FDIC regions.

FDIC management agreed with both recommendations, noting that it has begun quality assurance reviews of documentation prepared by FDIC examiners for examinations of TSPs in the MDPS program where the FDIC is the Agency-in-Charge. Further, the FDIC agreed to emphasize the importance of documenting adequate conclusions for key security control areas.

TABLE OF CONTENTS

FIGURES

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

Office of Audits
Office of Inspector General

DATE: November 30, 2007

MEMORANDUM TO: Sandra L. Thompson, Director
Division of Supervision and Consumer Protection

/Signed/
FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Examination Procedures for Assessing Selected Controls Related to the Protection of Customer and Consumer Information at Multi-regional Data Processing Servicers (MDPS)* (Report No. AUD-08-002)

This report presents the results of our third audit in a series of audits relating to the FDIC's oversight of technology service providers (TSP).[1] The overall purpose of these audits is to assess the FDIC's examination coverage of TSPs and related efforts to protect the customer and consumer information[2] of FDIC-supervised financial institutions. The objective of this audit was to assess the FDIC's implementation of the Federal Financial Institutions Examination Council (FFIEC)[3] and FDIC examination guidance for selected controls related to the protection of customer and consumer information at TSPs in the MDPS program. This audit focused on TSP controls in the following areas: (a) the oversight of TSP agreements with third-party service providers that maintain customer and consumer information; (b) response programs for addressing security incidents involving customer and consumer information; and (c) the disposal of customer and consumer information. We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix I discusses our audit objective, scope, and methodology in detail. Appendix III contains a glossary of terms.

BACKGROUND

FDIC-insured financial institutions are increasingly turning to TSPs to outsource critical information technology (IT) services, such as deposit and general ledger processing, check processing and imaging, and Web hosting. Frequently, these outsourcing

[1] See Appendix I for a description of the scope and objectives for the two prior audits.

[2] Customer information refers to records containing nonpublic personal information about a customer, that is, someone who has a continuing relationship (e.g., savings account or loan) with a financial institution. Consumer information refers to records about an individual that, in general, are derived from consumer reports. See Appendix III for further information related to these terms.

[3] The FFIEC is an interagency body statutorily empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the FDIC, the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA).

arrangements involve the collection, processing, and storage of customer and consumer information on behalf of financial institutions. While outsourcing offers financial institutions a number of important benefits, such as competitive advantages and cost-efficiencies, it also requires that appropriate steps be taken to ensure that TSPs adequately protect customer and consumer information in their custody. Widely publicized reports of data security breaches involving sensitive personal information[4] have raised concerns among banking regulators, the public, and the Congress, and underscore the importance of implementing sound security controls to protect customer and consumer information.

Requirements for Protecting Customer and Consumer Information

Two key statutes aimed at protecting sensitive personal information and preventing identity theft are the Gramm-Leach-Bliley Act (GLBA) of 1999 and the Fair and Accurate Credit Transaction Act of 2003 (FACT Act).

- GLBA states that it is congressional policy that financial institutions have an affirmative and continuing obligation to protect the security and confidentiality of their customers' non-public personal information. The statute directs the FDIC and other regulatory agencies to establish appropriate standards for the security and confidentiality of customer records and information pertaining to financial institution customers.

- The FACT Act, which amends the Fair Credit Reporting Act, is intended to protect consumers against the risks of identity theft and other types of consumer fraud by requiring that "any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose properly dispose of any such information or compilation." The Act directs the FDIC and other regulatory agencies to promulgate rules regarding the proper disposal of consumer information.

The FDIC, in coordination with the other regulatory agencies, implemented its responsibilities under GLBA and the FACT Act through the *Interagency Guidelines Establishing Information Security Standards* (the Security Guidelines).[5] The Security Guidelines require that financial institutions implement a comprehensive information security program that is designed, in general, to ensure the security, confidentiality, and proper disposal of customer and consumer information. A fundamental component of the security program is the development of a written risk assessment that addresses risks to the institution's customer and consumer information and the methods the institution uses

[4] In June 2005, it was reported that a security breach at a TSP exposed more than 40 million credit card accounts to potential fraud. In May 2007, it was reported that a financial services firm had discarded documents containing sensitive customer financial information in garbage bags outside of several of the firm's branch locations.

[5] Appendix B of Part 364 and Subpart I of Part 334 of the FDIC's Rules and Regulations. The Security Guidelines, effective July 1, 2001, implement sections 501(b) and 505 of GLBA and were amended effective July 1, 2005 to reflect section 216 of the FACT Act. The Security Guidelines set forth standards pursuant to section 39 of the Federal Deposit Insurance Act regarding, in general, safeguards to protect customer information.

to access, collect, store, use, transmit, protect, or dispose of such information. According to the Security Guidelines, financial institutions must take the following steps in assessing risk to their customer and consumer information:

- identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or consumer information systems;[6]

- assess the likelihood and potential damage of identified threats, taking into consideration the sensitivity of customer information; and

- assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control identified risks.

The Security Guidelines also state that financial institutions must address certain security control areas when developing and implementing their information security programs. Three of these security control areas were the focus of our audit:

- **Oversight of Service Providers.** Financial institutions shall (a) exercise appropriate due diligence when selecting service providers; (b) require service providers, by contract, to implement appropriate measures designed to meet the objectives of the Security Guidelines;[7] and (c) where indicated by the institution's risk assessment, monitor service providers to confirm that they have met their obligations to satisfy objectives of the Security Guidelines.

- **Response Programs.** Financial institutions must consider implementing a response program (including customer notification procedures) that specifies actions to be taken when unauthorized access to customer information systems is suspected or detected, including appropriate reports to regulatory and law enforcement agencies.

- **Disposal of Information.** Financial institutions must develop, implement, and maintain appropriate measures to properly dispose of customer and consumer information.[8]

The Security Guidelines recognize that when a financial institution enters into an outsourcing arrangement with a TSP, the institution continues to be responsible for the security of any customer or consumer information handled by the TSP on behalf of the institution. According to the Security Guidelines, financial institutions are expected to contractually require their service providers to implement appropriate measures designed to meet the objectives of the Security Guidelines.

---

[6] Any methods used to access, collect, store, transmit, protect, or dispose of customer information.

[7] By July 1, 2003, financial institutions were expected to include a requirement in all service provider contracts to maintain the security and confidentiality of customer information.

[8] Financial institutions were expected to comply with the disposal provisions of the Security Guidelines by July 1, 2005 and to modify all affected service provider contracts by July 1, 2006.

Federal Oversight of TSPs

The Bank Service Company Act authorizes the FDIC, FRB, and OCC to examine the operations of third-party companies that provide services to financial institutions.[9] The purpose of conducting such examinations is to identify and assess risks, including risks to the security of customer and consumer information, which may adversely affect the safety and soundness of serviced financial institutions. The FFIEC has published a series of IT Booklets (see Figure 1), collectively referred to as the *FFIEC IT Examination Handbook*, that contain guidance and procedures to assist examiners in conducting examinations of financial institutions and their TSPs. Examiners may tailor the procedures in the booklets based on examiner judgment and relevant examination factors, such as the size and complexity of the TSP and the quality of the TSP's risk assessment. For example, less work by examiners would be needed for a TSP that has thoroughly considered the risks to the security of its customer and consumer information as part of its risk assessment. Our audit assessed the FDIC's implementation of relevant examination procedures in IT Booklets 1-8 because these eight IT Booklets contain examination procedures related to the three security control areas covered by our audit.

Figure 1: IT Booklets That Comprise the *FFIEC IT Examination Handbook*

1. *Supervision of Technology Service Providers*
2. *Business Continuity Planning*
3. *Audit*
4. *Development and Acquisition*
5. *Outsourcing Technology Services*
6. *Management*
7. *Operations*
8. *Information Security*
9. *E-Banking*
10. *FedLine*
11. *Retail Payment Systems*
12. *Wholesale Payment Systems*

Source: FFIEC.

The FDIC issued examination guidance in its April 5, 2005 Regional Director Memorandum entitled, *Examination Procedures to Evaluate Response Programs for Unauthorized Access to Customer Information and Customer Notice*. The FDIC also issued two Financial Institution Letters (FIL)[10] relevant to the scope of our audit: the *Fair and Accurate Credit Transaction Act of 2003 Guidelines Requiring the Proper Disposal of Consumer Information* (dated February 2, 2005) and the *Risk Management of Technology Outsourcing* (dated November 29, 2000). We considered the guidelines in the memorandum and FILs in conducting our audit.

[9] Specifically, the bank regulator with jurisdiction over the principal investor of the bank service corporation may examine that service corporation or may authorize other bank regulators that supervise any other member of the service corporation to conduct the examination. Moreover, the Examination Parity and Year 2000 Readiness for Financial Institutions Act authorizes the OTS to examine service providers. The NCUA does not have statutory authority over service providers.

[10] The FDIC issues FILs to financial institutions to announce new regulations and policies, new FDIC publications, and other matters of interest to those responsible for operating a financial institution.

The MDPS Program

Certain TSPs, because of the high risk they pose to the financial services industry, are subject to interagency examination under the FFIEC's MDPS program. According to the FFIEC, disruptions in services, as a result of financial or operational conditions, at one of these TSPs pose systemic risk[11] to the banking system. The FFIEC considers a TSP for the MDPS program when the TSP processes critical applications, such as general ledger or loan and deposit systems, for a large number of financial institutions with multiple federal regulators or geographically dispersed data centers. As of June 25, 2007, there were 16 TSPs in the MDPS program, which collectively provide mission-critical IT services to the majority of the country's regulated financial institutions.

The FFIEC IT Subcommittee[12] has implemented a risk-based approach for determining the frequency and scope of examination coverage of TSPs in the MDPS program. Generally, TSPs in the MDPS program are subject to on-site examinations at least every 2 years and more frequently when supervisory concerns exist. On-site examinations are supplemented with interim reviews of material changes in TSP activities or condition. The scope and frequency of interim reviews vary, depending on the degree of change at the TSP, but are generally conducted at least once between on-site examinations. The FFIEC IT Subcommittee designates an Agency-in-Charge for each TSP in the MDPS program to coordinate examination activities. As of June 25, 2007, the FDIC was the Agency-in-Charge for 8 of the 16 TSPs in the MDPS program. The Agency-in-Charge is responsible for preparing key examination products, such as the scoping memorandum and Report of Examination (ROE). The scoping memorandum contains the TSP's corporate history, data centers included in the examination, examination schedule, and resource requirements. The ROE contains relevant examination findings, conclusions, and management comments and includes an IT examination rating reflecting the overall level of supervisory attention warranted for the TSP.[13]

FDIC's Oversight of TSPs in the MDPS Program

Within the FDIC, the Division of Supervision and Consumer Protection (DSC) has primary responsibility for examinations of TSPs in the MDPS program. In this capacity, DSC has taken a number of proactive measures. Of particular note, DSC hosted conferences in March 2006 and February 2007 with representatives of other FFIEC agencies to discuss issues, trends, and supervisory strategies related to TSPs in the MDPS program. DSC also implemented the *Technology Service Provider Event and Reporting Program* in June 2007 to assist FDIC examiners in analyzing pertinent financial,

[11] Systemic risk can occur when one participant fails to meet its obligations, causing other participants to fail to meet their obligations. Such a chain reaction can threaten the stability of financial markets.

[12] The IT Subcommittee, which is a standing committee of the FFIEC Task Force on Supervision, serves as a forum to address information systems and technology issues as they relate to financial institutions in order to promote quality, consistency, and effectiveness in examination practices.

[13] Examiners use the FFIEC's Uniform Ratings System for Information Technology to assess and rate IT-related risks at TSPs. Ratings are based on a scale of 1 through 5 in ascending order of supervisory concern, with 1 representing the highest rating and least degree of supervisory concern and 5 representing the lowest rating and highest degree of supervisory concern.

technical, and operational information pertaining to TSPs in the MDPS program. In addition, DSC continues to provide financial institutions with relevant information regarding the protection of customer and consumer information processed by TSPs through FILs, outreach initiatives (including conferences and speaking engagements), and the FDIC's public Web site.

RESULTS OF AUDIT

The FDIC has taken a number of proactive steps in its oversight of TSPs in the MDPS program. During our audit, the FDIC hosted the *2007 FFIEC MDPS Supervisory Strategy Meeting*, enhanced its monitoring of TSPs in the MDPS program, and conducted a number of outreach initiatives. Importantly, FDIC examiners use FFIEC and FDIC examination guidance when assessing security controls related to the protection of customer and consumer information at TSPs in the MDPS program. Additionally, as part of each examination, the examiners considered the risk assessment for security controls prepared by the TSP in response to the Security Guidelines. However, the risk assessments for the three TSPs we reviewed generally did not address the three security control areas (oversight of TSP third-party service providers, incident response programs, and the disposal of information) covered by our audit, and examination documentation we reviewed generally did not contain conclusions on security risks in these control areas. As a result, we were unable to determine whether related examination procedures performed at the three TSPs we reviewed were commensurate with the risk of unauthorized access to customer and consumer information.

Providing conclusions in FDIC examination documentation on the risks for key security control areas related to the protection of customer and consumer information would promote consistency in security control assessments performed by the FDIC's regional offices for TSPs in the MDPS program. Such information would also be valuable to examiners when they assume examination responsibilities for TSPs in the MDPS program, such as when examination responsibilities transition from one regulator to another. In addition, enhanced linking of examination procedures with identified security risks would provide DSC greater assurance that customer and consumer information processed by TSPs in the MDPS program is protected consistent with the statutory and regulatory requirements intended to safeguard such information.

ASSESSING SECURITY RISKS RELATED TO THE PROTECTION OF CUSTOMER AND CONSUMER INFORMATION

The *FFIEC IT Examination Handbook* states that examiners should evaluate the degree of risk and the quality of risk management as part of each TSP examination. This involves, among other things, reviewing the TSP's internally-prepared risk assessment to evaluate the organization's practices for identifying, measuring, controlling, and monitoring security risks. Evaluating TSP risk assessments helps examiners focus examination resources on the TSP control areas that present the greatest risk. For the

three TSPs we sampled, we noted that examiners were evaluating the adequacy of TSP-prepared risk assessments. However, neither the TSP-prepared risk assessments nor the examination documentation (e.g., working papers, ROEs, and scoping memoranda) adequately described the security risks in the three control areas covered by our audit. In addition, the scope of examination procedures performed in these three control areas varied significantly among the TSPs we reviewed. As a result, we were unable to determine whether the examination procedures performed in these three control areas were commensurate with the associated security risks.

The following sections describe the varying degree of examination coverage related to the oversight of service providers, response programs, and the disposal of information.

Oversight of Service Providers. The FFIEC's *Outsourcing Technology Services* IT Booklet defines four fundamental control areas associated with the outsourcing of IT services by financial institutions or TSPs: *Risk Assessment and Requirements*, *Service Provider Selection*, *Contract Issues*, and *Ongoing Monitoring*. The IT Booklet contains examination guidance, objectives, and procedures to assist examiners in assessing risks (including security risks) in each of the four IT outsourcing control areas. Figure 2 summarizes the examination objectives associated with each IT outsourcing control area as described in the *Outsourcing Technology Services* IT Booklet. In addition, the FFIEC's *Information Security* IT Booklet contains guidance and examination procedures for evaluating security controls associated with the oversight of service providers.

Figure 2: Examination Objectives for Evaluating the Oversight of Service Providers

- *Risk Assessment and Requirements:* Evaluate the quantity of risk present from the outsourcing arrangement and the quality of risk management.
- *Service Provider Selection*: Evaluate the service provider selection process.
- *Contract Issues*: Evaluate the process for entering into a contract with the service provider.
- *Ongoing Monitoring*: Evaluate the process for monitoring the risk presented by the service provider relationship. Review the policies regarding periodic ranking of service providers by risk for decisions regarding the intensity of monitoring (i.e., risk assessment).

Source: OIG Analysis of the FFIEC's *Outsourcing Technology Services* IT Booklet.

Although examiners considered each of the four IT outsourcing control areas in Figure 2 when examining TSPs in the MDPS program, the scope of examination procedures performed in these areas to assess security risks varied significantly. For example, with respect to *Risk Assessment and Requirements*, examination working papers for two of the three TSPs we reviewed did not include procedures to determine whether the TSP had identified all of its service providers with access to customer and consumer information. Identifying service providers with access to customer and consumer information is a critical step in determining whether the service providers' security controls are consistent with the principles of the Security Guidelines. Regarding *Contract Issues*, examination working papers for two of the three TSPs did not contain procedures to assess the adequacy of security requirements in service provider contracts. In addition, examination

working papers for one of the three TSPs did not contain procedures to assess security in the areas of *Service Provider Selection* or *Ongoing Monitoring*.

Response Programs. In March 2005, the FDIC, in coordination with the other FFIEC agencies, issued supplemental guidance regarding GLBA and the Security Guidelines[14] by describing five minimum components of a response program that financial institutions should develop and implement to address incidents of unauthorized access to sensitive customer information (see Figure 3). The Security Guidelines state that financial institutions must require their service providers, by contract, to implement appropriate security measures for responding to incidents of unauthorized access to customer information. In addition, DSC's April 5, 2005 memorandum entitled, *Examination Procedures to Evaluate Response Programs for Unauthorized Access to Customer Information and Customer Notice*, contains procedures to assist FDIC examiners in evaluating and documenting the five components of a response program.

Figure 3: Components of a Response Program

1. Assessing the nature and scope of the incident and identifying the systems and types of information that have been accessed.
2. Taking appropriate steps to contain and control the incident.
3. Notifying the institution's primary federal regulator.
4. Notifying appropriate law enforcement authorities if a *Suspicious Activity Report* is filed.
5. Notifying customers, when warranted.

Source: The Security Guidelines.

Although examiners performed procedures to address all five components of a response program at two of the three TSPs we reviewed, examiners did not perform examination procedures to address two of the five response program components at the remaining TSP. Specifically, examiners did not perform procedures to determine whether the TSP had adequate controls in place for notifying federal regulators of incidents involving unauthorized access to, or use of, customer information. In addition, examiners did not perform procedures to fully assess the role and responsibilities of a key TSP contractor involved in assessing, containing, and controlling security incidents.

Disposal of Information. The Security Guidelines direct financial institutions to require their service providers, by contract, to implement appropriate measures to protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to customers. Such measures include developing, implementing, and maintaining appropriate controls for disposing of customer and consumer information processed on behalf of financial institutions. Examples of "reasonable measures" that organizations and individuals can take when disposing of consumer information are provided in the Federal Trade Commission's regulation, *Disposal of*

[14] The FDIC's version of the supplemental guidance appears as Supplement A, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, to Appendix B of Part 364.

Consumer Report Information and Records (the Disposal Rule).[15] In addition, the FFIEC's *Business Continuity Planning*, *Information Security*, and *Operations* IT Booklets contain examination guidance and procedures for assessing security controls related to the disposal of information. The FFIEC examination guidance and procedures can be divided into three areas: (1) assessing disposal risks; (2) reviewing and evaluating the sufficiency of security policies and standards related to disposal; and (3) determining whether disposal controls and processes are appropriately implemented.

Although examiners conducted procedures to review and evaluate security policies and standards related to the disposal of information at all three of the TSPs we reviewed, procedures for assessing the implementation of those policies and standards varied. At one of the TSPs, the internal audit department conducted extensive work on an outside disposal firm engaged by the TSP to destroy information,[16] and the examiners included the review results in the examination working papers. Although the remaining two TSPs had also engaged outside disposal firms, the internal audit department at those two TSPs did not perform comprehensive procedures, and the examiners did not assess key controls related to TSP disposal operations. In addition, examination working papers for two of the three TSPs did not include procedures to assess disposal risks associated with known security vulnerabilities, such as inadequate controls over sensitive records and a lack of encryption for data stored on back-up tapes, laptop computers, and personal digital assistants.

How the FDIC Can Achieve Greater Assurance That Conclusions on Risks for Key Security Control Areas Are Included in Examination Documentation

The FFIEC's *Supervision of Technology Service Providers* IT Booklet states that examination working papers must provide sufficient documentation for a reviewer to understand what work was done, why it was done, and how conclusions were reached. However, FFIEC and FDIC examination guidance does not describe how conclusions on security risks related to the protection of customer and consumer information should be recorded in the examination documentation. FDIC examination staff that we spoke with indicated that requiring FDIC examiners to include information in the examination documentation regarding their conclusions on risks for key security control areas would be beneficial. Examiners noted that such information would promote consistency in TSP security control assessments among the FDIC's regional offices. Examiners also noted that such information would be valuable to examiners when they assume examination responsibilities for TSPs in the MDPS program, such as when examination responsibilities transition from one regulator to another. In addition, through enhanced

[15] 16 Code of Federal Regulations (C.F.R.) Part 682. Such measures include, for example, conducting due diligence of prospective disposal firms by reviewing an independent audit of the disposal company's operations and/or its compliance with the Disposal Rule, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the disposal company. The Disposal Rule became effective June 1, 2005.

[16] The work included, but was not limited to, (a) confirming that shredder bins were locked; (b) inquiring whether the disposal firm had been certified by the National Association for Information Destruction, Inc.; and (c) obtaining representations that disposals were supervised and that destruction logs were maintained.

linking of examination procedures performed with identified security risks, DSC would have greater assurance that customer and consumer information processed by TSPs in the MDPS program is protected consistent with statutory and regulatory requirements that are intended to safeguard such information.

DSC can further strengthen its oversight of TSPs in the MDPS program by subjecting underlying FDIC examination documentation, including working papers, to a periodic quality assurance review. DSC has already established and implemented a formal quality assurance program to promote consistency and quality in its risk-management, compliance, and IT examination processes. However, DSC has not yet conducted a quality assurance review of FDIC examination working papers related to TSPs in the MDPS program. Such quality assurance reviews would provide DSC with greater assurance that examination documentation adequately addresses risk determinations for key security control areas related to the protection of consumer and customer information, procedures are performed commensurate with identified risk, and examination processes are consistently applied across FDIC regions.

Recommendations

We recommend that the Director, DSC:

(1) Provide conclusions on the risks for key security control areas in FDIC examination documentation for examinations of TSPs in the MDPS program in order to provide greater assurance that examination procedures performed are commensurate with identified risks.

(2) Conduct periodic quality assurance reviews of examination documentation prepared by FDIC examiners under the MDPS program to achieve greater assurance that MDPS examination documentation contains risk determinations for key security control areas, procedures performed are commensurate with identified risk, and examination processes are consistently applied across FDIC regions.

CORPORATION COMMENTS AND OIG EVALUATION

On November 21, 2007, the Director, DSC, provided a written response to a draft of this report. DSC's response is presented in its entirety as Appendix IV to this report. DSC agreed with both recommendations, noting that it has begun incorporating quality assurance reviews of documentation prepared by FDIC examiners for examinations of TSPs in the MDPS program where the FDIC is the Agency-in-Charge. Further, DSC agreed to emphasize the importance of documenting adequate conclusions for key security control areas.

DSC's actions are responsive to our recommendations. A summary of management's response to the recommendations is in Appendix V. The recommendations are resolved but will remain open until we have determined that agreed-to corrective actions have been completed and are effective.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of the audit was to assess the FDIC's implementation of FFIEC and FDIC examination guidance for selected controls related to the protection of customer and consumer information at TSPs in the MDPS program. We conducted this performance audit from December 2006 through July 2007 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Scope, Methodology, and Internal Controls

The audit focused on the implementation of FFIEC and FDIC examination guidance in the following three security control areas relative to customer and consumer information processed by TSPs in the MDPS program on behalf of FDIC-insured financial institutions:

- the oversight of TSP agreements with third-party service providers that maintain customer and consumer information;
- response programs for addressing security incidents involving customer and customer information; and
- the disposal of customer and consumer information.

We selected these three security control areas for review because of recent media, regulatory, and industry attention.

To obtain an understanding of FFIEC examination guidance in the three security control areas, we reviewed relevant IT Booklets in the *FFIEC IT Examination Handbook*, particularly, the *Supervision of Technology Service Providers* and *Information Security* IT booklets. We also reviewed relevant FDIC examination guidance contained in DSC's April 5, 2005 Regional Director Memorandum entitled, *Examination Procedures to Evaluate Response Programs for Unauthorized Access to Customer Information and Customer Notice*. In addition, we reviewed relevant FILs, including *Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Consumer Information* (dated February 2, 2005) and *Risk Management of Technology Outsourcing* (dated November 29, 2000). Further, we reviewed relevant information posted on the FDIC's internal and public Web sites. To obtain an understanding of the FDIC's supervisory oversight of TSPs in the MDPS program, we interviewed DSC Technology Service Branch personnel who had responsibility for establishing and maintaining the FDIC's IT examination policies, procedures, and guidance and for coordinating with representatives of the FFIEC IT Subcommittee. Additionally, we interviewed DSC

regional office personnel to obtain an understanding of MDPS examination strategies, staffing, and practices.

We assessed the FDIC's implementation of FFIEC and FDIC examination guidance by selecting a non-statistical sample[17] of three TSPs in the MDPS program for which the FDIC was the Agency-in-Charge. Each TSP was under the supervisory oversight of a different DSC regional office. One of the three TSP examinations we reviewed processed $1.5 trillion in payments daily, another TSP provided information processing for over 500 clients, and the third TSP serviced over 4 million merchant locations. For each TSP, we conducted a detailed review of the examination documentation, including the underlying working papers and key examination products, such as the scoping memorandums and ROEs. Additionally, we spoke with the Examiners-in-Charge and other key FDIC examination staff regarding their examination approach for addressing the three security control areas covered by our audit. Further, we spoke with representatives of the U.S. Government Accountability Office regarding security control work it had conducted at one of the TSPs in our review.

We did not speak with examination staff at other federal banking regulators who had performed examination work on the three TSPs we reviewed. In addition, we did not visit any TSP offices or speak with TSP representatives. We conducted our audit work at the FDIC's Headquarters offices in Washington, D.C.; the Dallas Regional Office in Dallas, Texas; the Kansas City Regional Office in Kansas City, Missouri; and the New York Regional Office in Manhattan, New York.

Reliance on Computer-based Data

We did not assess the reliability of the FFIEC's computer-based data or the FDIC's Virtual Supervisory Information On the Net system (ViSION)[18] information because the data were not significant to our findings, conclusions, or recommendations.

Compliance with Laws and Regulations

We evaluated whether IT examination procedures to assess selected controls related to the protection of customer and consumer information at TSPs in the MDPS program were adequate to address relevant provisions of GLBA, the FACT Act, and the Security Guidelines. We used certain other federal regulations, such as the Federal Trade Commission's *Standards for Safeguarding Customer Information* and *Disposal of Consumer Report Information and Records* (16 C.F.R. Parts 314 and 682, respectively), as supplemental criteria. Our assessment was limited to the three security control areas covered by our audit (i.e., the oversight of TSP third-party service providers, incident response programs, and the disposal of information). Accordingly, our assessment did

[17] The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

[18] ViSION is a bank-supervision tracking and reporting database. DSC refers to ViSION as an "information workstation" – a programmed means of handling all the computerized data needed to properly supervise an institution throughout its organizational life.

not generally include the FDIC's regulations at Part 332, *Privacy of Consumer Financial Information*, which implements GLBA's provisions regarding privacy notices and related disclosures with respect to customers and consumers, except where definitions in Part 332 were referred to or incorporated in the Security Guidelines. See Appendix II for additional information on relevant laws and regulations, including their legal effect on the FDIC.

Government Performance and Results Act

We reviewed the FDIC's *Strategic Plan for 2005-2010* and the *FDIC 2007 Annual Performance Plan.* Neither of these plans contained a strategic goal or objective specifically related to examinations of TSPs in the MDPS program. We also reviewed the FDIC's *2007 Corporate Performance Objectives* (CPO) and determined that it did not contain a specific CPO related to our audit objectives. However, the first quarter CPO performance summary stated that a separate effort was underway to assess the potential risk associated with outsourcing to third-party TSPs, with a focus on TSPs based in foreign countries. According to the performance summary, the FDIC has developed a tool to collect data on a quarterly basis from FDIC-supervised institutions on their use of such TSPs.

Fraud and Illegal Acts

The nature of our audit objective did not require that we develop specific audit procedures to detect fraud and illegal acts. However, throughout the audit, we were sensitive to the potential for fraud and illegal acts, and no indications of fraud or illegal acts came to our attention.

Prior Coverage

This audit is the third in a series of audits designed to assess the FDIC's examination coverage of TSPs and related efforts to protect customer and consumer information. The first audit, *FDIC's Oversight of Technology Service Providers* (OIG Audit Report No. 06-015, dated July 2006), focused on the FDIC's efforts to identify, monitor, and prioritize examination coverage of TSPs. The second audit, *Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers* (OIG Audit Report No. 07-005, dated February 2007), focused on examination procedures related to the security of customer information managed by TSPs. We considered the results of these prior audits when planning and conducting our current audit work.

APPENDIX II

LAWS, REGULATIONS, POLICY, AND GUIDANCE

Laws	**Provisions**
Gramm-Leach-Bliley Act (GLBA)	Title V of the Act contains provisions to protect nonpublic personal information of financial institution customers. It is congressional policy that each financial institution has an obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. Each agency (including the FDIC) or authority should establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.
Bank Service Company Act	A bank service company shall be subject to examination and regulation by the appropriate federal banking agency of its principal investor to the same extent as its principal investor. The Act requires insured financial institutions to notify their appropriate federal banking agency, in writing, of contracts or relationships with third parties that provide certain services to the institution. The depository institution shall notify such agency of the existence of the service relationship within 30 days after making the service contract or the performance of the service, whichever occurs first.
Fair Credit Reporting Act (FCRA)	This statute regulates the collection, dissemination, and use of consumer credit information.
Fair and Accurate Credit Transactions Act of 2003 (FACT Act)	This statute, which amends FCRA, requires federal regulators, including the FDIC, to issue regulations in a number of areas, including regulations on the disposal of consumer information (section 216).
Federal Deposit Insurance Act, section 39	This provision requires the federal banking agencies to prescribe standards for financial institutions in a number of areas, as well as operational and managerial standards as deemed appropriate.
Rules & Regulations	
12 C.F.R. Part 334, Subpart I - *Duties of Users of Consumer Reports Regarding Identity Theft*	These FDIC regulations require institutions to properly dispose of any consumer information in accordance with the Security Guidelines.

12 C.F.R. Part 364, *Standards for Safety and Soundness,* Appendix B, *Interagency Guidelines Establishing Information Security Standards*[19] Appendix B, Supplement A, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*	These are the FDIC's version of interagency guidelines which, among other things, address the proper disposal of consumer information requirements pursuant to section 628 of the FCRA and apply to all insured state nonmember banks, insured state licensed branches of foreign banks, and any subsidiaries of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisers). Supplement A provides guidance for institutions regarding response plans, including customer notification procedures.
16 C.F.R. Part 314, *Federal Trade Commission (FTC) – Standards for Safeguarding Customer Information* (Safeguards Rule)	The Safeguards Rule sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. The rule applies to the handling of customer information by all financial institutions over which the FTC has jurisdiction. Financial institutions subject to this rule must also require their service providers, by contract, to implement and maintain the safeguards discussed in this rule.
16 C.F.R. Part 682, *FTC – Disposal of Consumer Report Information and Records* (Disposal Rule)	The Disposal Rule requires any person who maintains or otherwise possesses consumer information for a business purpose to properly dispose of such information by taking reasonable measures to protect against unauthorized access to, or use of, the information in connection with its disposal. The rule provides several examples of reasonable measures, which include incorporating the proper disposal of consumer information into the information security program required by the FTC Safeguards Rule.
Guidance	
FIL 81-2000, *Risk Management of Technology Outsourcing*	The FIL provides joint guidance from the FFIEC regulators on managing the risk exposure an institution faces when it uses outside firms for technology. Specifically, the regulators issued guidance on key management issues involved in outsourcing technology, including risk assessment, service provider selection, contract terms, and oversight of outsourcing arrangements.
FIL-68-2001, 501(b), *Examination Guidance*	Examination procedures described in the guidance are derived from the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* and are intended to assist examiners in assessing the level of compliance with the guidelines.
FIL 7-2005, *Guidelines Requiring the Proper Disposal of Consumer Information.*	The bank and thrift regulatory agencies issued joint final guidelines to implement section 216 of the FACT Act. Section 216 is designed to protect consumers against the risks associated with identity theft and other types of fraud. This final rule amended *Interagency Guidelines Establishing Standards for Safeguarding Customer*

[19] These Standards were revised effective July 1, 2005 and were re-titled, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.*

	Information to require proper disposal of consumer information. This rule also requires financial institutions to modify any affected contracts with service providers no later than July 1, 2006.
FIL-27-2005, *Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*	The FFIEC agencies jointly issued guidance for financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive customer information maintained by the financial institution or its service provider. The guidance is an interpretation of section 501(b) of GLBA and the *Interagency Guidelines Establishing Information Security Standards.*
Regional Directors Memoranda	
RD-90-116, *Problem Electronic Data Processing Centers*	Contains instructions for the supervision of a problem electronic data processing center. A problem center is any servicer that has been assigned a composite "4" or "5" rating under the Uniform Interagency Rating System for Data Processing Operations.
RD-93-086, *EDP Examinations of Non-Financial Institution Data Centers*	Provides guidance on scheduling an interagency examination of data centers operated by independent servicers, bank service corporations, or financial institution holding companies. Data centers included in the MDPS program are administered by the Electronic Data Processing (EDP) Subcommittee of the FFIEC's Task Force on Supervision.
RD-95-013, *Enhanced Supervision Program for MDPSs*	Details the Enhanced Supervisory Program for MDPSs, which has been approved by the FFIEC Task Force on Supervision.
RD-00-026, *Examination of National Data Processing Companies*	Supplements the *EDP Interagency Examination, Scheduling, and Distribution Policy* (Supervisory Policies, SP-1 and SP-11) and provides for coordination, standardization, and unification needed for the examination of MDPSs.
RD-00-032, *Scheduling of Information Systems Examinations*	Establishes a centralized listing of data center examinations that may require participation by other regions.
RD-01-032, *Examination Procedures to Evaluate Customer Information Safeguards*	Provides examination procedures to determine compliance with the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* (Appendix B to Part 364 of the FDIC Rules and Regulations) that were mandated by Section 501(b) of the GLBA to address standards for financial institutions in the development and implementation of administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer records and information.
RD-01-039, *Guidelines for Examination Workpapers and Discretionary Use of Examination Documentation Modules*	Provides guidelines on preparing examination workpapers. Examination findings should be documented through a combination of brief summaries, bank source documents, report comments, and other papers that address management practices and conditions.

	Documentation should provide written support for examination and verification procedures performed and conclusions reached.
RD-04-002, *Establishing Standards for Safeguarding Customer Information*	Provides guidance on reporting the results of evaluating a financial institution's compliance with the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.*
RD-04-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*	Explains the effective dates of the provisions in the Fair and Accurate Credit Transactions Act of 2003 and provides guidance regarding the impact of these dates on compliance and IT examination programs.
RD-05-012, *Examination Procedures to Evaluate Response Programs for Unauthorized Access to Customer Information and Customer Notice*	Details examination procedures to determine compliance with the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*.
RD-04-059, *Information Technology Examination Quality Control*	Contains an update to the IT examination documentation requirements.
RD-06-013, *IT – Risk-Based Examination Priority Ranking Program*	Announces the Risk-Based Examination Priority Ranking Program procedures for all TSPs, including providers in the MDPS program.

GLOSSARY OF TERMS

Term	Definition
Consumer	An individual or the legal representative of such an individual who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes.
Customer	With respect to a financial institution, any person (or authorized representative of a person) to whom the financial institution provides a product or service, including that of acting as a fiduciary.
Consumer Information	Any record about an individual, whether in paper, electronic, or other form.
Consumer Information Systems	Any methods used to access, collect, store, transmit, protect, or dispose of customer information.
Customer Information	Any information maintained by or for a financial institution that is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer.
Data Breach	Generally refers to an organization's unauthorized or unintentional exposure, disclosure, or loss of sensitive personal information, which can include personally identifiable information such as Social Security numbers or financial information such as credit card numbers. Data breaches can take many forms and do not necessarily lead to identity theft.
Disposal	The act of discarding media with no other sanitization considerations. This is done by paper recycling containing non-confidential information but may also include other media. Disposal also includes the discarding or abandonment of consumer information or the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.
Encryption	A process that scrambles the contents of a message or file to make it unintelligible to anyone who is not authorized to read it.
Identity Theft	Identity theft is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name. Depending on the type of information compromised and how it is misused, identity theft victims can face a range of potential harm, from the inconvenience of having a credit card reissued to substantial financial losses and damaged credit ratings.
Incident	An incident can be a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Incidents include denial of service, malicious code, unauthorized access, and inappropriate usage.

Incident Notification	When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, the institution should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. Customer notification should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it, such as by telephone, regular mail, or electronic mail (for those customers for whom it has a valid e-mail address) and who have agreed to receive communications electronically.
Media	Media take different forms, such as printouts of data, screenshot captures, or cached memory of users' activities.
Multi-regional Data Processing Servicer (MDPS)	A TSP qualifies for the MDPS program when the TSP processes critical applications, such as general ledger or loan and deposit systems, for a large number of financial institutions with multiple federal regulators or geographically dispersed data centers.
Nonpublic Personal Information	Nonpublic personal information means: (1) personally identifiable financial information; and (2) any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.
Report of Examination (ROE)	The ROE is the joint property of the FFIEC member agencies and contains two sections. The open section contains an assessment of major risks to the financial institutions serviced by the MDPS, recommendations for reducing or managing those risks, and management's responses to the findings and recommendations. The MDPS's directors sign and date the Directors' Signature Page as certification that they have reviewed the ROE. The open section is furnished to the MDPS. The Uniform Rating System for Information Technology -- or IT examination rating -- included in the administrative section is available only to supervisory agencies.
Response Program	Response programs specify actions to be taken when a financial institution suspects or detects that unauthorized individuals have gained access to customer information systems. The program should contain procedures for the following: a. Assessing the nature and scope of an incident and identifying which customer information systems and types of customer information have been accessed or misused. b. Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to, or use of, sensitive customer information. c. Notifying appropriate law enforcement authorities and filing a timely *Suspicious Activity Report* in situations involving federal criminal violations requiring immediate attention.

	d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to, or use of, customer information. e. Notifying customers when warranted.
Scoping Memorandum	A document that provides details on the organization, scope of the upcoming examination, data centers to be included in the examination, examination schedule, and resource requirements. The document, which is submitted to the FFIEC IT Subcommittee for approval, identifies the risks highlighted in the last examinations and areas for further review and outlines the examination's objectives, assignments, workday budget, and other relevant information.
Sensitive Customer Information	Sensitive customer information is a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information, such as user name or password or password and account number, that would allow someone to log onto or access the customer's account.
Service Provider	Any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through its provision of services directly to a financial institution.
Technology Service Provider (TSP)	TSPs include independent data centers, including MDPSs, joint venture/limited liability corporations, and bank service corporations.

CORPORATION COMMENTS

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

DATE: November 21, 2007

TO: Russell A. Rau
Assistant Inspector General for Audits

FROM: Sandra L. Thompson [signed]
Director

SUBJECT: Response to Draft Report Entitled: ***Examination Procedures for Assessing Selected Controls Related to the Protection of Customer and Consumer Information at Multi-regional Data Processing Servicers (MDPS) 2006-040***

This memorandum represents the Division of Supervision and Consumer Protection (DSC) response to the draft report entitled, *Examination Procedures for Assessing Selected Controls Related to the Protection of Customer and Consumer Information at Multi-regional Data Processing Servicers (MDPS)* prepared by the FDIC's Office of Inspector General (OIG). This audit focused on FDIC's implementation of FFIEC and FDIC examination guidance for selected controls related to the protection of customer and consumer information at technology service providers (TSP) in the MDPS program. The OIG draft report concluded that FDIC has taken a number of proactive steps in its oversight of TSPs in the MDPS program including hosting the 2007 FFIEC MDPS Supervisory Strategy Meeting, enhanced its monitoring of TSPs in the MDPS program, and conducted a number of outreach initiatives. Additionally, as part of each examination, the examiners considered the risk assessment for security controls prepared by the TSP in response to the Security Guidelines. DSC's actions to address each recommendation are discussed below.

OIG Recommendations:

1. **Provide conclusions on the risks for key security control areas in FDIC examination documentation for examinations of TSPs in the MDPS program in order to provide greater assurance that examination procedures performed are commensurate with identified risks.**

   DSC Response:
   DSC concurs that conclusions regarding security controls at Technology Service Providers in the MDPS program, where the FDIC is the Agency-in-Charge (AIC), should be clearly documented when examined as provided for in the FFIEC IT Examination Handbooks. DSC will emphasize to the FDIC regions the importance of documenting adequate conclusions for key security control areas by March 28, 2008.

2. **Conduct periodic quality assurance reviews of examination documentation prepared by FDIC examiners under the MDPS program to achieve greater assurance that MDPS examination documentation contained risk determinations for**

key security control areas; procedures performed are commensurate with identified risk; and examination processes are consistently applied across FDIC regions.

DSC Response:
DSC concurs that MDPS examinations should include a periodic quality assurance review. This would serve to strengthen our MDPS program and related examination documentation. In order to promote consistency across all FDIC regions, the Technology Services Branch in October, 2007, initiated the inclusion in their scope of regional office reviews, a quality assurance review of examination documentation prepared by FDIC examiners where FDIC is the AIC.

MANAGEMENT RESPONSE TO RECOMMENDATIONS

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

Rec. No.	Corrective Action: Taken or Planned	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	DSC will emphasize to the FDIC regions the importance of documenting adequate conclusions for key security control areas.	March 28, 2008	$0	Yes	Open
2	DSC has begun quality assurance reviews of documentation prepared by FDIC examiners for examinations of TSPs in the MDPS program where the FDIC is the Agency-in-Charge.	October 2007	$0	Yes	Open

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

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