Office of Inspector General

July 2006
Report No. 06-015

FDIC's Oversight of Technology Service Providers

AUDIT REPORT

Office of Audits

OIG

Office of Audits

Report No. 06-015
July 2006

FDIC's Oversight of Technology Service Providers

Background and Purpose of Audit

Under the Bank Service Company Act (BSCA), the FDIC and other federal financial regulators have statutory authority to regulate and examine the services a technology service provider (TSP) performs for FDIC-insured financial institutions.

According to the Federal Financial Institutions Examination Council (FFIEC) *Outsourcing Technology Services Handbook*, TSP relationships should be subject to the same risk management, security, privacy, and other internal controls and policies that would be expected if the financial institution were conducting the activities directly.

The overall objective for our series of audits of the FDIC's oversight of TSPs is to assess the FDIC's examination coverage of TSPs and related efforts to protect sensitive customer information. For this audit, we assessed the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage of TSPs. We also reviewed the extent to which TSP information was being captured in the FDIC's Virtual Supervisory Information On the Net system (ViSION).

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

Results of Audit

The FDIC actively supported the FFIEC through examinations of numerous high-priority TSPs and has acted to strengthen its Information Technology (IT) Risk Management Program and coverage of TSPs. However, the FDIC's oversight process used for identifying, monitoring, and prioritizing TSPs for examination coverage needs improvement. The FDIC does not have a current, accurate, and complete inventory of TSPs that are used by FDIC-supervised institutions and have access to sensitive customer information. The FDIC has taken action to address known weaknesses related to the TSP inventory, but additional attention is needed, particularly for TSPs that process sensitive customer information. Additionally, our evaluation of TSP data in ViSION found that the Division of Supervision and Consumer Protection (DSC) had not implemented adequate controls to obtain and maintain TSP data. As a result, the FDIC's ability to identify and monitor TSPs; assess risk, including risk related to sensitive customer information; and prioritize use of examination resources for financial institutions and TSPs is limited.

Also, the FDIC could improve its participation in the TSP risk-based supervisory process used by the federal banking agencies. The FDIC was not always obtaining and completing Examination Priority Ranking Sheet (EPRS) information, which is used in scheduling and prioritizing TSP examinations in accordance with FFIEC guidance. In addition, FFIEC guidance on ranking TSPs as part of the EPRS process did not address consideration of the TSPs' processing of sensitive customer information. As a result, FFIEC decisions and FDIC input into those decisions on the risks posed by TSPs and the frequency and extent of TSP examinations could lack sufficient support.

Recommendations and Management Response

The report makes six recommendations to help the FDIC: (1) better identify and monitor TSPs with access to sensitive customer information and (2) improve the process the FDIC uses (in conjunction with the other FFIEC agencies) for assessing the risks posed by, and prioritizing for examination, those TSPs with access to sensitive customer information.

FDIC management generally agreed with our recommendations. The FDIC will take steps to improve its TSP inventory and sharing of TSP information with the other federal banking agencies, enhance controls over BSCA notifications, increase data reliability, and work with the FFIEC IT Subcommittee regarding including in the new risk-based examination priority ranking program those TSPs processing sensitive customer information.

TABLE OF CONTENTS

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

Office of Audits
Office of Inspector General

DATE: July 20, 2006

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

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

SUBJECT: *FDIC's Oversight of Technology Service Providers*
(Report No. 06-015)

This report presents the results of the first in a series of audits of the FDIC's oversight of technology service providers (TSP).[1] We initiated this audit in response to reported data security breaches in 2005 involving sensitive customer information[2] maintained by financial institutions and, in some cases, TSPs (see Appendix III). The overall objective for our series of audits on TSPs is to assess the FDIC's examination coverage of TSPs and related efforts to protect sensitive customer information. For this audit, we assessed the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage. Appendix I of this report details our objective, scope, and methodology.

BACKGROUND

Under the Bank Service Company Act (BSCA),[3] the FDIC and other federal financial regulators have statutory authority to regulate and examine the services performed by third parties, such as TSPs for FDIC-insured financial institutions. The FDIC's Division of Supervision and Consumer Protection (DSC) has designated two categories of information technology (IT) examinations for providing examination coverage of TSPs. For TSPs that are owned or controlled by, or otherwise affiliated with, an FDIC-supervised financial institution, examination coverage is provided through DSC's IT examination of the institution. The IT examination is generally conducted in coordination with safety and soundness examinations. For examinations

[1] According to *Interagency Guidelines Establishing Information Security Standards* (Appendix B to Part 364 of the FDIC Rules and Regulations), service provider—"means any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank."

[2] Sensitive customer information is defined by Appendix B to Part 364 of the FDIC Rules and Regulations as a customer's social security number, personal identification number, password, or account number, in conjunction with a personal identifier such as the customer's name, address, or telephone number. Such information would also include any combination of components of customer information that would allow someone to log onto or access another person's account, such as a user name and password.

[3] Codified to 12 U.S.C. 1867. Section 7(c) of the BSCA requires FDIC-insured financial institutions to notify the appropriate federal regulator of the existence of a third-party relationship within 30 days after contracting with, or the performance of the service by, the third party, whichever occurs first.

of TSPs designated as Independent Data Centers (IDCs),[4] DSC policy directs the use of guidance issued by the FDIC and the other federal banking agencies that are members of the Federal Financial Institutions Examination Council (FFIEC).[5] This guidance, which describes a risk-based supervisory approach for IT examinations of TSPs, prioritizes the IDCs based on risk, with the FFIEC considering those TSPs rated a higher risk for separate IT examinations (discussed below). The relationships with lower-risk TSPs can receive examination coverage through the review of the financial institution's vendor management program. We did not assess examination coverage of vendor management as part of this audit, but we are currently conducting an audit of that examination function.

The FFIEC IT examination handbook entitled, *Supervision of Technology Service Providers* (TSP Handbook), identifies four work products related to separate IT examinations of TSPs.

- **TSP Examination** - The FFIEC agencies examine the higher-risk IDCs, as defined earlier, to identify existing or potential risks that could adversely affect serviced financial institutions. As of March 31, 2005 (the latest data available), there were approximately 130 of these TSPs subject to periodic examination, and the FDIC was the Agency-in-Charge (AIC) for 88 of those TSPs.

- **Multi-Regional Data Processing Servicer (MDPS) Examination** - A TSP is considered for the MDPS program if it processes mission-critical applications, such as general ledger or loan and deposit systems, for a large number of financial institutions with multiple regulators or geographically dispersed data centers. For example, some MDPSs process mission-critical applications for more than 1,000 financial institutions. FFIEC guidance requires examinations of MDPSs every 2 years or less, depending on the level of supervisory concern, because these entities pose a systemic risk to the banking system should one or more have operational problems or fail. Prior to September 30th of each year, the FFIEC Information Technology Subcommittee[6] of the Task Force on Supervision determines a schedule of MDPS examinations, which are performed jointly by the agencies. As of March 31, 2005, 17 TSPs were in the MDPS program.

- **Shared Application Software Review (SASR)** - A SASR is an interagency review of software programs or systems used by numerous financial institutions. SASRs help to reduce the time and resources needed to examine software and systems at individual institutions.

- **Follow-Up Review** - The purpose of this review is to: maintain communications with TSPs between on-site examinations; identify significant changes in management, products, services, or risk management practices affecting financial institutions; follow

[4] IDCs are defined by the FDIC as TSPs that are not owned or controlled by, or otherwise affiliated with, a financial institution.
[5] In addition to the FDIC, the FFIEC includes the Federal Reserve Board, National Credit Union Administration, Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).
[6] Representative IT examiners from the five FFIEC member agencies comprise this subcommittee.

up on issues or concerns previously identified; and confirm business-line or service provider risk designations and their examination priority in order to update supervisory strategies.

The FFIEC has stated that the use of a TSP does not diminish the responsibility of the financial institution's board of directors and management to ensure that the activities performed by the TSP are conducted in a safe and sound manner and in compliance with applicable laws and regulations. According to the FFIEC *Outsourcing Technology Services Handbook* (Outsourcing Handbook), TSP relationships should be subject to the same risk management, security, privacy, and other internal controls and policies that would be expected if the financial institution were conducting the activities directly. According to the Outsourcing Handbook, written contracts are required for all outsourced servicing arrangements, including those with financial institution affiliates.

Section 501 of the Gramm-Leach-Bliley Act (GLBA)[7] requires the federal banking agencies to establish appropriate standards for financial institutions subject to their supervision in order to protect the security and confidentiality of customer information. The Act generally prohibits any financial institution from disclosing information to nonaffiliated third parties without notice to, and an opportunity for, the customer to opt out. The Act also provides an exception for nonaffiliated third parties, such as TSPs, that perform services for or functions on behalf of the financial institution. In response to the GLBA, the federal banking agencies issued *Interagency Guidelines Establishing Information Security Standards*, found at Appendix B of Part 364 of the FDIC Rules and Regulations. These guidelines require a financial institution to have a comprehensive information security program that includes safeguards appropriate to the size and complexity of the institution and nature and scope of its activities. Under these guidelines, banks must (1) require their TSPs, by contract, to implement appropriate measures to meet the objectives of the guidelines related to protecting against unauthorized access to or use of sensitive customer information and (2) monitor contract compliance by the TSPs, where warranted, according to the institution's assessment of risk.

The FFIEC's TSP Handbook identifies the risks associated with maintaining the confidentiality and integrity of information. For example, the TSP Handbook discusses the reputational risk associated with errors, delays, or omissions in information technology that become public knowledge or directly affect customers and the compliance risk associated with the unauthorized disclosure of customer information that could expose institutions to civil money penalties or litigation. To capture information on these and other risks, the TSP Handbook recommends the use of an Examination Priority Ranking Sheet (EPRS) for those TSPs subject to separate IT examinations. The FFIEC agencies use this information to determine supervisory priorities based on the TSP's business line risks, client base, and adequacy of internal control and risk management practices.

DSC uses the Virtual Supervisory Information On the Net (ViSION) system to provide automated support for many aspects of bank supervision, including application tracking, case management, safety and soundness examination, information technology examination, offsite

[7] See Appendix II for a summary of laws, regulations, and guidance pertaining to data security at FDIC-insured institutions and related privacy requirements.

monitoring, large bank analysis, management reporting, workload management and processing, and security. ViSION is used to capture information on examinations of financial institutions and their TSPs, including technology profiles and related risk data.

RESULTS OF AUDIT

The FDIC actively supported the FFIEC through examinations of numerous high-priority TSPs and has acted to strengthen its IT Risk Management Program and coverage of TSPs. However, the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and prioritizing TSP examination coverage needs improvement.

The FDIC does not have a current, accurate, and complete inventory of TSPs that are used by FDIC-supervised institutions and have access to sensitive customer information. The FDIC has taken action to address known weaknesses related to the TSP inventory, but additional attention is needed, particularly for TSPs that process sensitive customer information. Additionally, our evaluation of TSP data in ViSION found that DSC had not implemented adequate controls to obtain and maintain TSP data. As a result, the FDIC's ability to identify and monitor TSPs; assess risk, including risk related to sensitive customer information; and prioritize use of examination resources for financial institutions and TSPs is limited (Finding A).

The FDIC also could improve its participation in the TSP risk-based supervisory process used by the federal banking agencies. The FDIC was not always obtaining and completing EPRS information used in scheduling and prioritizing TSP examinations in accordance with FFIEC guidance. In addition, FFIEC guidance on ranking TSPs as part of the EPRS process did not address consideration of the TSPs' processing of sensitive customer information. As a result, FFIEC decisions and FDIC input into those decisions on the risks posed by TSPs and the frequency and extent of TSP examinations could lack sufficient support (Finding B).

FINDINGS AND RECOMMENDATIONS

Finding A: Inventory of TSPs

DSC does not have a current, accurate, and complete inventory of TSPs that are used by FDIC-supervised institutions and have access to sensitive customer information. Instead, the inventory is largely limited to those TSPs that are subject to separate examinations under FFIEC guidelines. In addition, TSP-related data, including data related to TSP processing of sensitive customer information, needed to perform thorough risk assessments and make fully informed decisions on examination priorities is not readily available for use in support of the TSP examination process. The primary causes of this condition are (1) outdated guidance to institutions on BSCA compliance, (2) no formal requirement for examiners to assess the adequacy of institution compliance with BSCA notification requirements, and (3) weaknesses in controls for obtaining and maintaining TSP data in the ViSION system from both BSCA notifications and IT examinations. As a result, the FDIC's ability to identify and monitor TSPs; assess risk, including as it relates to sensitive customer information; and prioritize use of examination resources for financial institutions and TSPs is limited.

BSCA Institution Guidance. The FDIC has not established adequate internal controls to ensure that information on all TSP relationships is obtained. Specifically, in June 1999, the FDIC issued a Financial Institution Letter (FIL-49-99, *Required Notification for Compliance with the Bank Service Company Act*) reminding institutions of applicable BSCA notification requirements. The FIL further noted that some institutions were neglecting to file the required BSCA notices. The FIL contained an optional notification form that could be used by institutions in reporting covered contracts and relationships. The FIL used language from the BSCA to identify the types of services covered by the Act, but offered little clarification as to how that language should be interpreted and applied to contracts and other relationships for more recently implemented technology-related services. No other FILs addressing BSCA compliance have been issued to institutions since 1999, despite advances in technology-related services and increased use of TSPs by institutions. The BSCA was enacted on October 23, 1962, and the definition of services in Section 3 of the Act predates certain activities currently performed by TSPs, such as those related to Internet banking. As discussed below, inconsistent reporting of TSP relationships could result from varying interpretations of the BSCA notification requirement. Also, there is no requirement in the FIL or under the BSCA for a bank to notify the FDIC when a third-party service relationship is terminated. However, additional guidance to banks, including a requirement to notify the FDIC when a TSP relationship is terminated, would help provide necessary control for routine or consistent BSCA notifications to the FDIC that would support maintenance of a current, accurate, and complete TSP inventory.

Further, there are indications that financial institutions may be continuing to enter into BSCA-covered relationships with TSPs without providing required notices to the FDIC. For example, one TSP we identified performed credit card processing for five institutions supervised by the FDIC. In accordance with the BSCA, these five institutions should have filed BSCA notifications with the FDIC, describing, among other things, the services performed by the TSP. However, DSC could not locate copies of the BSCA notifications for four of the five institutions. According to DSC officials in San Francisco, some confusion exists among banks regarding the scope and applicability of the BSCA, and banks are not always notifying the FDIC of their third-

party service relationships. Based on our interviews with DSC officials, no additional information pertaining to the BSCA notifications has been issued to banks since the 1999 FIL.

While updating and reissuing the 1999 FIL would help in addressing the concerns noted in this report, the FDIC should consider regulatory and other options, together with the other federal banking agencies, in order to ensure that BSCA notifications and the TSP inventory are current, accurate, and complete. In addition to providing notification of new contracts or service agreements with TSPs, such options could include uniform reporting on all TSP relationships using standard data elements for BSCA notifications, processing of sensitive customer information, information on third-party reviews and other oversight of TSPs,[8] publicly available information such as financial statements of the TSP,[9] and identification and notification of terminated TSP relationships.

BSCA-Related Examination Guidance and Data Validation. Current guidance issued to DSC examiners on assessing the adequacy of institution compliance with BSCA notification requirements is insufficient. Under DSC's former *Information Technology General Work Program*, issued in April 2004, examiners were required to determine whether the financial institution had filed notifications on TSP relationships with the appropriate regulator, as required by the BSCA, for services outsourced since the previous examination. However, this guidance was superseded in August 2005 by IT examination guidance on the FDIC's Information Technology – Risk Management Program (IT-RMP). This IT examination guidance does not require examiners to determine a bank's compliance with the BSCA notification requirements. Also, the current guidance does not require examiners to validate TSP information in the ViSION IT Examination Module, which serves as the TSP inventory and tracking system. Such validation should include use of both the BSCA notifications and IT examination information related to TSPs, as discussed below. Examination coverage of compliance with BSCA notification requirements and validation of the TSP data maintained by DSC in ViSION are critical to ensuring that the FDIC has a current, accurate, and complete TSP inventory; TSP data are reliable; and all TSP relationships are properly considered in the supervisory process.

Obtaining and Maintaining IT Examination Data on TSPs. Our evaluation of TSP data in ViSION found that DSC had not implemented adequate controls to obtain and maintain TSP data. Specifically, we found numerous problems with the integrity of data relating to TSPs, including duplication, incomplete data fields, and listings of TSP relationships that are no longer active. Further, we noted that ViSION's ability to perform information queries is limited. For example, ViSION does not have the capability of listing banks serviced by a particular TSP or all the TSPs that are providing services to a particular financial institution. These issues reduce the usefulness of ViSION as a management tool for identifying and monitoring potential risks presented by TSPs and for prioritizing examination coverage.

[8] Part 364 of the FDIC Rules and Regulations discusses financial institution oversight of service provider relationships, including monitoring audits and other reviews of TSPs. This oversight is intended to help ensure that institutions and their service providers are meeting the *Interagency Guidelines Establishing Information Security Standards*, which require an appropriate information security program to be in place to protect customer information.

[9] In an article in the (summer 2005) FDIC *Supervisory Insights*, the FDIC noted the benefits of the review and analysis of public information in developing the Corporation's supervisory response to potential risks at TSPs.

As part of the IT examination process established in IT-RMP, examiners are required to complete a Technology Profile Script (Profile Script) on each financial institution and to obtain from the institution an Officer's Questionnaire to help identify risks posed by the institution's IT program, including risks posed by TSPs. The Profile Script is designed to be a basic measurement of the complexity and potential risk of the technology deployed at a financial institution. The Profile Script is not designed to identify all TSPs used by the institution. Because of the focus on institution risk, the Profile Script requires only limited information, such as the TSP name, for those TSPs processing core banking applications and providing Web site hosting and transactional E-Banking. TSPs used by institutions to perform other functions, such as credit card and mortgage processing, are not addressed in the Profile Script. Additionally, the Profile Script does not assign a priority to TSPs that process sensitive customer information or otherwise require collection of this data. As a result, the Profile Script is not a source of complete information on TSPs providing services to a particular financial institution or processing sensitive customer information. According to DSC officials, the primary focus of the Profile Script is to determine the level of expertise needed to examine the institution. We also noted that the Officer's Questionnaire requests information about the institution's IT program with a focus on information security but does not request information on all TSPs servicing the institution or on TSPs that process sensitive customer information.

After completing an IT examination of a financial institution, examiners are required to complete an IT ViSION database for each type of system or platform[10] maintained by or for the financial institution. An IT template is the source of TSP data for ViSION. However, the template does not provide for capturing information on all TSPs, only those considered a higher risk by the examiner-in-charge of the examination. As a result, ViSION contains limited information to help the FDIC assess the risks related to the security of sensitive customer information at TSPs.

We performed an initial query of TSP information in ViSION and found over 10,000 records, many of which were duplicate records or contained outdated information. DSC informed us that the information was not accurate and provided us with a revised database reflecting approximately 800 TSP records. DSC officials informed us that when the conversion from the legacy system[11] to ViSION occurred in 2005, some of the TSP information was lost and errors were introduced. According to DSC officials, it will take some time to ensure that the ViSION database contains all the appropriate technology profiles of financial institutions and TSPs. ViSION is the primary source for completing the Profile Script used in pre-examination planning. Therefore, the completeness and reliability of the data is critical to upcoming examinations that can include TSP coverage.

We also found that ViSION has limited reporting capabilities for TSPs. Although reports of TSPs can be retrieved, queries of this information are limited. For example, due to a system glitch and incomplete data, queries cannot be performed on a specific TSP and the services it

[10] A "platform" describes some sort of framework, either in hardware or software, that allows software to run. Typical platforms include a computer's architecture, operating system, or programming languages and their runtime libraries.

[11] The Banking Information Tracking System was previously used by DSC to track financial institution information.

provides to financial institutions. Therefore, DSC did not use ViSION to monitor or prioritize TSPs for examination coverage. Further, DSC information received through BSCA notifications was not entered into ViSION.

Finally, DSC is maintaining a separate tracking system for BSCA notifications. As previously stated, the information from these notifications is not being entered into ViSION. Rather, since November 2004, DSC has required regional offices to send BSCA notices submitted by institutions to the DSC Technology Supervision Branch in Washington, D.C., where the information is entered into a separate "stand-alone" database that is not linked directly to ViSION. DSC implemented this procedure to have a centralized system for tracking BSCA notifications. As of December 2005, the Washington, D.C., database included information on BSCA notifications from about 400 of the more than 5,000 financial institutions that the FDIC supervises. At present, DSC does not use this information as part of the examination process to determine the risks posed by individual TSPs to financial institutions. The justification for maintaining two separate systems to track TSP data is not clear, especially given that the BSCA database is not used for supervisory purposes. In our opinion, the oversight process for TSPs requires the integration of information received through BSCA notifications and as a result of examinations rather than the maintenance of separate systems that are not reliable or fully utilized.

DSC has the responsibility for ensuring the reliability of data in ViSION and its other information systems. FDIC Circular 1301.3, *Data Stewardship Program*, establishes the objectives of that program, including ensuring the usefulness, accuracy, timeliness, and accessibility of corporate data. The circular indicates that the FDIC's divisions and offices shall ensure that data stewardship responsibilities are fulfilled, including those related to the reliability of data. For DSC, this responsibility should include maintaining a current, accurate, and complete inventory of TSPs used by financial institutions and related information in order to successfully manage both safety and soundness risk and ensure the protection of sensitive customer information. For example, some of the key risk factors in determining risk associated with a TSP are the size of its client base, aggregate assets affected, and transaction volume. Without an accurate system to identify and monitor TSPs, including information on how many institutions a particular TSP services and which TSPs process sensitive customer information, the risk assessment process that identifies TSPs for examination is limited.

RECOMMENDATIONS

We recommend that the Director, DSC:

(1) Assess, in conjunction with the other federal banking agencies, regulatory and other options for establishing and maintaining a current, accurate, and complete inventory of TSP information through the use of BSCA notifications, examination results, and other available data. Consideration should be given specifically to the content of BSCA notifications, the initiation and termination of TSP relationships, third-party reviews and other oversight of TSPs, and the processing of sensitive customer information.

(2) Revise IT examination guidance to address coverage of financial institution compliance with BSCA notification requirements.

(3) Establish policy and procedures for updating ViSION with information from BSCA notifications and the results of IT examinations, and discontinue use of a separate database for tracking these notifications.

(4) Establish controls as part of DSC's implementation of the FDIC Data Stewardship Program to ensure the reliability and usefulness of TSP data in ViSION. Consideration should specifically be given to:

- Modifying the Profile Script, Officer's Questionnaire, and IT ViSION Template to identify all TSPs used by a financial institution and the relevant risk factors, including those that process sensitive customer information.

- Validating, as part of the supervisory process, TSP information in the ViSION IT Examination Module.

- Enhancing the ViSION report retrieval process to allow for the retrieval of information by TSP, to include data on all financial institutions serviced, as well as by institution, to include all TSPs used.

Finding B: Obtaining and Completing EPRS Information

The FDIC's participation in the risk-based supervisory process of TSPs used by the federal banking agencies could be improved. The FDIC was not always obtaining and completing EPRS information used in scheduling and prioritizing TSP examinations in accordance with FFIEC guidance. In addition, FDIC guidance does not address the agencies' consideration of the TSPs' processing of sensitive customer information when ranking TSPs as part of the EPRS process. As a result, FFIEC decisions and FDIC input into those decisions on the risks posed by TSPs and the frequency and extent of TSP examinations could lack sufficient support.

The EPRS Process. To assist in scheduling and prioritizing TSP examinations, the FFIEC agencies use EPRSs. The EPRS assigns various supervisory priorities to TSPs based on the relative risk of their business lines, client base, and overall controls and risk management oversight. TSPs determined to be higher risk are subject to more frequent and extensive examinations and reviews. The AIC, as designated by the FFIEC, is responsible for coordinating the risk ranking of each TSP under its supervision. The TSP Handbook requires that at the conclusion of each TSP examination, the AIC is responsible, in part, for completing applicable sections of the EPRS for each TSP and then distributing the form for review and comment by other agencies. The risk-ranking factors are analyzed and discussed by the federal banking agencies comprising the FFIEC to determine future examination priority. The EPRS provides a framework for grouping TSPs into various supervisory priorities, based on the relative risk of their business lines, client base, and their overall controls and risk management.

The TSP Handbook provides for an interagency review process that distributes sections of the completed EPRSs and allows for agency agreement or disagreement to be communicated and documented. In particular, the TSP Handbook states that the AIC is responsible for the following:

- Distributing copies of the completed sections of the EPRS to the other FFIEC agencies.
- Collecting agency agreements/disagreements and resolving any priority disagreements to the extent possible.
- Retaining all documentation supporting the priority designation and agency agreement/disagreement.
- Documenting the basis for the disagreement in the comment section of the EPRS when a resolution cannot be reached.

Further, the TSP Handbook states that agency representatives receiving an EPRS from the AIC are responsible for:

- Reviewing the completed sections of the EPRS.
- Completing the *Agency Agreement on Examination Priority* section and providing necessary comments, as applicable.
- Returning the completed form to the AIC by the requested response date.
- Retaining a copy for their records.

Obtaining and Completing EPRS Information. We reviewed the San Francisco Regional Office's (SFRO) *Service Provider Profile Manual*, which contains information on 28 TSPs.[12] Our review showed the following:

- The EPRSs were not completed as required at the conclusion of each TSP examination. The EPRSs showing FDIC as the designated AIC had not been updated or reanalyzed since July 2002, despite subsequent TSP examinations. The EPRSs for which the FDIC was not the AIC were not always dated, which raised questions about current applicability.

- EPRSs were not always obtained from other regulatory agencies. In three out of six instances for which the FDIC was not the AIC, an EPRS was not obtained from the other regulatory agency. The only documentation retained, in two of these cases, was the SFRO's own data and analysis.

- For those TSPs for which the FDIC was not the AIC, the FDIC's concurrence was not always annotated within the EPRSs, and no supporting documentation was maintained justifying the FDIC's position or signifying that the FDIC had communicated its position to the AIC.

Also, supporting documentation was not being maintained to signify interagency agreement or disagreement and decisions on key sections of the EPRSs. For those TSPs for which the FDIC was the AIC, interagency concurrence was annotated in the EPRSs. However, no supporting documentation (such as a letter, e-mail, or meeting minutes) was maintained that signified interagency concurrence.

We noted that supervisory personnel are not required to identify the analytical basis used for completing the EPRS, such as results from an off-site analysis, other reviews, or a TSP examination. We noted that in those areas where documentation guidelines exist, FDIC personnel are not sufficiently documenting and/or supporting interagency concurrence. The EPPRs we reviewed did not note the source of the data used and analyzed, and oftentimes did not note the date that the EPRS had been completed. Although some EPRSs did not indicate that a supervisory review had occurred, regional office officials typically annotated when a supervisory review had been completed for those TSPs for which the FDIC was the AIC.

Examiners manually complete EPRSs and maintain them in various file folders at the regional offices. This manual process does not facilitate the sharing of information within the FDIC or with the other federal banking agencies, data monitoring and analysis, or timely updates. An automated EPRS process would be beneficial for updating EPRSs and for facilitating the regional office review and coordination processes with other federal banking agencies. A

[12] Of these 28 TSPs, 19 were listed in the SFRO TSP examination plan for 2004-2005. The FDIC was the AIC for 7 of the 19 TSPs, another agency was the AIC for 6 TSPs, and joint examinations were conducted on 6 TSPs designated as MDPSs. For those seven TSPs for which the FDIC was the AIC, six TSPs (86 percent) had a completed EPRS. For the one TSP that had an incomplete EPRS, a note attached to the form indicated that no ranking sheet was needed. However, no further explanation was provided, even though this TSP continues to be examined.

modification to automatically complete EPRSs in ViSION, which is already capturing some of the information needed for an EPRS, may assist the FDIC in its supervision of TSPs.

FDIC Guidance on the EPRS Process. The SFRO has implemented several practices that have enhanced its use of EPRSs and supervisory oversight for TSPs. In particular, the SFRO compiled information sheets that documented and centralized supporting data on certain TSPs. These sheets typically captured information on a TSP's ownership structure, system/software specifications, examination history, customer asset size, and a customer listing. The SFRO also maintained a service provider profile manual, which served as a central file for all completed EPRSs. Additionally, the SFRO performed and documented a review of those EPRSs. Furthermore, the SFRO maintains a TSP examination planning spreadsheet to facilitate examination tracking and scheduling. These best practices on the part of the SFRO should be considered by the FDIC for implementation across DSC because they helped to ensure adequate support for the EPRS process.

However, neither the SFRO nor the Atlanta Regional Office considered the processing of sensitive customer information a significant factor in completing an EPRS. The EPRS focuses on client base, business lines, prior examination rating, effective external oversight, technological stability, and prior problems in deciding upon risk factors. Notwithstanding, the FDIC can and should ensure that the risks associated with processing sensitive customer information are factored into its recommendations to the FFIEC on the supervisory approach for a particular TSP. The FDIC had not issued guidance as a supplement to the TSP Handbook regarding the consideration of processing sensitive customer information as a risk factor for the EPRS. As a result, decisions by the FFIEC and FDIC concerning the risks posed by TSPs and the frequency and extent of TSP examinations could lack sufficient support.

RECOMMENDATIONS

We recommend that the Director, DSC:

(5) Issue supplemental guidance to the TSP Handbook on the completion and sharing of EPRSs among the federal banking agencies and the consideration of the TSPs' processing of sensitive customer information in assigning risk factors to the TSPs.

(6) Assess the merits of implementing an automated process, including the use of ViSION, for collecting, storing, monitoring, and sharing EPRSs and other TSP-related information with the other federal banking agencies comprising the FFIEC.

CORPORATION COMMENTS AND OIG EVALUATION

On July 19, 2006, the Acting 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. The Acting Director indicated that the FDIC has long recognized that the protection of sensitive customer information by either financial institutions or service providers is a significant consumer protection and safety and soundness risk area.

In its response, DSC generally agreed with the recommendations, noting that it had already implemented or considered many of the recommendations and will work with the FDIC's interagency partners to enhance the FDIC supervisory programs for TSPs. Regarding the TSP inventory, DSC agreed that the FDIC would benefit from enhancing centralized collection of TSP data. Further, DSC will assess its options for improving the accuracy and completeness of the inventory of TSP information and will vet the TSP inventory issues raised in this report with the other FFIEC agencies. DSC also agreed that its IT examination procedures would include an option for a compliance review of BSCA and has already included such a review in the IT General Work Program. Additionally, DSC will review the IT officer's questionnaire for appropriate inclusion of BSCA notification requirements.

DSC indicated that the data integrity issues with ViSION were the result of an upgrade and conversion from the prior legacy system to ViSION. During 2005, DSC implemented a data correction process, and by the end of that year, had a high level of confidence in the database. Nevertheless, DSC will review its TSP controls and consider opportunities for further enhancement. DSC will propose to develop a centralized collection system to add BSCA notifications to the ViSION architecture. DSC will also include a self-assessment item for BSCA notification requirements in the officer's questionnaire, evaluate and consider additional risk-ranking measures for TSPs, and propose relevant findings to the FFIEC IT Subcommittee for consideration. DSC noted that the current ViSION report capability allows it to report all TSPs for a given institution and all institutions serviced by a given TSP. While we agree that the capability exists, continuing problems with uploading customer lists (which show the number of banks serviced by a TSP) into ViSION have limited DSC's ability to generate accurate reports on TSPs. DSC is currently addressing this problem through its IT Committee. In our opinion, the steps DSC is taking are sufficient to meet the intent of our recommendation.

With respect to obtaining and completing EPRS information, DSC noted that a new risk-based examination priority ranking program has been adopted by the FFIEC, and the TSP Handbook is currently being rewritten to include new procedures. According to DSC, upon completion of the TSP Handbook, supervisory decisions about TSPs will have sufficient support. Also, DSC will raise the topic of including sensitive customer information in the risk-ranking process to the FFIEC IT Subcommittee for discussion and consideration. Further, DSC will forward the OIG recommendation of assessing the merits of implementing an automated process for collecting, storing, monitoring, and sharing TSP and specific risk-related information among the federal banking agencies to the FFIEC IT Subcommittee for discussion and consideration.

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

OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective for our series of audits of the FDIC's oversight of TSPs is to assess the FDIC's examination coverage of TSPs and related efforts to protect sensitive customer information. For this audit, we assessed the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage. We focused our review on the FDIC's processes for identifying, monitoring, and prioritizing examinations of TSPs in light of the potentially significant data security risks these firms pose to consumers and the financial services industry. TSPs included in the MDPS program have been identified as entities that pose a systemic risk to the banking system and are examined periodically. Therefore, we did not review the process pertaining to the MDPS program. In addition, we limited our review to an evaluation of the adequacy of established policies and procedures and overall prioritization of TSPs and did not evaluate the performance of individual TSP examinations or other examinations that include TSP coverage.

We performed our audit from August 2005 through March 2006 in accordance with generally accepted government auditing standards. We reviewed selected TSP examinations and EPRSs that had been completed during 2004 and 2005. Additionally, we reviewed and analyzed:

- the BSCA and applicable guidance issued by the FDIC;
- various FDIC IT Examination Procedures and applicable Regional Director's Memoranda;
- the FFIEC's four information technology examination handbooks entitled, *Management, Outsourcing Technology Services, Supervision of Technology Service Providers*, and *Retail Payment Systems*;
- IT examination data in ViSION;
- DSC's *Security Incident Report* listings;
- the Multi-Regional Data Processing Servicers list;
- the SFRO's Technology Service Provider Examination listing and scheduling process;
- the SFRO's and Atlanta Regional Office's EPRSs and related procedures; and
- information files maintained at the San Francisco and Atlanta Regional Offices.

Additionally, we interviewed DSC officials in Washington, D.C., and in the San Francisco and Atlanta Regional Offices.

Government Performance and Results Act, Reliance on Computer-Processed Data, Management Controls, Compliance with Laws and Regulations, and Fraud and Illegal Acts

The Government Performance and Results Act of 1993 directs federal agencies to develop a strategic plan, align agency programs and activities with concrete missions and goals, manage and measure results, and design budgets that reflect strategic missions. In this audit, we reviewed the *FDIC's 2005 Annual Performance Plan* and the FDIC's *Strategic Plan for 2005-2010*. These plans do not specifically address the subject of our audit.

We conducted tests to determine the reliability of computer-processed data obtained from the FDIC's ViSION system. Based on the review of information in ViSION, the data were not current, accurate, and complete as discussed in the findings in this report.

We gained an understanding of relevant control activities by examining applicable policies and procedures as presented in the FDIC Rules and Regulations, FDIC's Statement of Policy, DSC's *Risk Management Manual of Examination Policies*, FDIC's *Case Manager Procedures Manual*, Examination Documentation Modules, and Regional Directors Memoranda and by reviewing available FFIEC and FDIC documentation related to TSP supervision and examination.

Regarding compliance with laws and regulations, we gained an understanding of aspects of the Federal Deposit Insurance (FDI) Act and the requirements of the FDIC Rules and Regulations. Also, we reviewed applicable sections of the BSCA. However, DSC documentation was not sufficient for us to verify institution compliance with the BSCA notice requirements (as discussed in this report). The scope of the audit did not encompass testing for fraud or illegal acts; nevertheless, we were alert for, but did not detect such activity.

Regarding how banks manage their TSP relationships, we limited our work to gaining an understanding of the information examiners obtain during bank examinations. Also, we did not include offshore outsourcing of technology services in the scope of our audit. Future audit coverage in this area will include detailed reviews of vendor management, TSP examinations, offshore outsourcing, and supervisory efforts that address compliance with laws and regulations pertaining to safeguarding sensitive customer information.

LAWS, REGULATIONS, AND GUIDANCE PERTAINING TO DATA SECURITY AT FDIC-INSURED INSTITUTIONS AND RELATED PRIVACY REQUIREMENTS

Laws	Provisions
12 United States Code (U.S.C.) 1464(d)(7) Home Owners' Loan Act	(A) General examination and regulatory authority. A service company or subsidiary that is owned in whole or in part, by a savings association shall be subject to examination and regulation by the Director, OTS, to the same extent as that savings association. (B) Examination by other banking agencies. The Director may authorize any other federal banking agency that supervises any other owner of part of the service company or subsidiary to perform an examination described in subparagraph (A). (D) Services performed by contract or otherwise. Notwithstanding subparagraph (A), if a savings association, a subsidiary thereof, or any savings and loan affiliate or entity, as identified by Section 8(b)(9) of the FDI Act, that is regularly examined or subject to examination by the Director, causes to be performed for itself, by contract or otherwise, any service authorized under this chapter or applicable state law, whether on or off its premises, (i) such performance shall be subject to regulation and examination by the Director to the same extent as if such services were being performed by the savings association on its own premises; and (ii) the savings association shall notify the Director of the existence of the service relationship not later than 30 days after the date on which the contract is entered or the date on which performance is initiated.
12 U.S.C. 1867 Bank Service Company Act	(a) Principal investor. 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 appropriate federal banking agency of the principal shareholder or principal member of such bank service company may authorize any other federal banking agency that supervises any other shareholder or member of the bank service company to make such an examination. (c) Services provided by contract or otherwise. Notwithstanding section (a) above, whenever a bank that is regularly examined by an appropriate Federal banking agency, or any subsidiary or affiliate of such a bank that is subject to examination by that agency, causes to be performed for itself, by contract or otherwise, any services

	authorized under this chapter, whether on or off its premises: (1) such performance shall be subject to regulation and examination by such agency to the same extent as if such services were being performed by the bank itself on its own premises, and (2) the bank shall notify such agency of the existence of the service relationship within 30 days after making such a service contract or the performance of the service, whichever occurs first.
15 U.S.C. 6801 Gramm-Leach-Bliley Act	Protection of nonpublic personal information. (a) Privacy obligation policy. It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. (b) Financial institutions' safeguards. In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for financial institutions subject to their jurisdiction 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 which could result in substantial harm or inconvenience to any customer.
Regulations	
12 Code of Federal Regulations (C.F.R.) Part 332 *Privacy of Consumer Financial Information*	(a) Purpose. Part 332 governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part: (1) Requires a financial institution to provide notice to customers about its privacy policies and practices. (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties. (3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§ 332.13, 332.14, and 332.15. (b) Scope. (1) Part 332 applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes. This part does not apply to information about companies or about individuals who obtain financial

	products or services for business, commercial, or agricultural purposes. This part applies to the United States offices of entities for which the FDIC has primary supervisory authority.
Fair Credit Reporting Regulations 12 C.F.R. Part 334	Interagency Proposed Rule implementing provisions of the Fair Credit Reporting Act (FCRA) that permit institutions to communicate consumer information to their affiliates without incurring the obligations of consumer reporting agencies. The privacy rule does not modify, limit, or supersede the operation of FCRA.
12 C.F.R. Part 364, Standards for Safety and Soundness, Appendix B, *Interagency Guidelines Establishing Information Security Standards*	(a) General standards. The Interagency Guidelines Establishing Standards prescribed pursuant to section 39 of the FDI Act (12 U.S.C. 1831p--1), as set forth as Appendix A to this part, apply to all insured state nonmember banks and to state-licensed insured branches of foreign banks that are subject to the provisions of section 39 of the FDI Act. (b) Interagency Guidelines Establishing Information Security Standards. These guidelines prescribed pursuant to section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831p--1), and sections 501 and 505(b) of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, 6805(b)), and with respect to the proper disposal of consumer information requirements pursuant to section 628 of the FCRA (15 U.S.C. 1681w), as set forth in Appendix B to this part, 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).
Guidance	
FIL-89-2004, *FFIEC Information Technology Examination Handbook*	The FFIEC has issued booklets with guidance on evaluating management and outsourcing technology services. The FIL states that "outsourcing of an activity does not relieve management and the board of directors of their responsibility to ensure the institution's data are processed in a secure environment and to maintain data integrity."
FIL-27-2004, *Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes*	The FDIC alerted financial institutions to the increasing prevalence of e-mail and Internet-related fraudulent schemes targeting financial institution customers. The guidance provides financial institutions with background information on these schemes and describes how institutions can assist in protecting their customers.

Fair and Accurate Credit Transactions (FACT) Act Implementation	The OCC, FDIC, and OTS are adopting a final rule to implement section 216 of the FACT Act by amending the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*. The final rule generally requires each financial institution to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports.
Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Y2000 Standards for Safety and Soundness 66 *Federal Register* 8615	Guidelines establishing standards for safeguarding customer information were revised to reference the security guidelines, implement Section 501(b) of GLBA, and require institutions to mandate appropriate security controls for contractual service providers.
FIL-64-2005, *Guidance on How Financial Institutions Can Protect Against Pharming Attacks*	The FDIC issued guidance to financial institutions describing the practice of "pharming," how it occurs, and potential preventive approaches. Financial institutions offering Internet banking should assess potential threats posed by pharming attacks and protect Internet domain names, which – if compromised – can heighten risks to the institutions.
FIL-49-99, *Bank Service Company Act*	Section 7(c)(2) of the Bank Service Company Act states that any FDIC-supervised institution that has services performed by a third-party "shall notify such agency of the existence of the service relationship within 30 days after the making of such service contract or the performance of the service, whichever occurs first." As defined in Section 3 of the Act, these services include "check and deposit sorting and posting; computation and posting of interest and other credits and charges; preparation and mailing of checks, statements, notices, and similar items; or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution."
FIL-50-2001, Bank Technology Bulletin: *Technology Outsourcing Information*	The bulletin introduces three short documents containing practical ideas for banks to consider when they engage in technology outsourcing. The documents are for informational purposes only and should not be considered examination procedures or official guidance.

SUMMARY OF FINANCIAL INSTITUTION AND TSP-RELATED DATA SECURITY BREACHES REPORTED IN 2005

Date Made Public	Institution Name	Type of Breach	Number of Consumers Affected
Feb. 15, 2005	ChoicePoint	Bogus accounts established by identity thieves	145,000
Feb. 25, 2005	Bank of America	Lost backup tape	1,200,000
Feb. 25, 2005	PayMaxx	Exposed online	25,000
April 20, 2005	Ameritrade	Lost backup tape	200,000
April 28, 2005	Wachovia, Bank of America, PNC Financial Services Group, and Commerce Bancorp	Dishonest insiders	676,000
May 16, 2005	Westborough Bank	Dishonest insider	750
June 6, 2005	CitiFinancial	Lost backup tapes	3,900,000
June 16, 2005	CardSystems Solutions, Inc.	Hacking	40,000,000
June 29, 2005	Bank of America	Stolen laptop	18,000
July 6, 2005	City National Bank	Lost backup tapes	Unknown
Aug. 30, 2005	J.P. Morgan	Stolen laptop	Unknown
Sept. 16, 2005	ChoicePoint (2nd notice, see Feb. 15 for 145,000)	ID thieves accessed; also misuse of IDs and passwords.	9,903
Sept. 17, 2005	North Fork Bank, NY	Stolen laptop with mortgage data	9,000
Sept. 23, 2005	Bank of America	Stolen laptop with information of Visa Buxx users (debit cards)	Not disclosed
Sept. 28, 2005	RBC Dain Rauscher	Illegitimate access to customer data by former employee	100+ customers' records compromised out of 300,000
Nov. 8, 2005	ChoicePoint	Bogus accounts established by ID thieves Total affected now 172,000 (See Feb. 15 & Sept. 16)	17,000 in addition to those noted earlier
Nov. 9, 2005	TransUnion	Stolen computer	3,623
Nov. 11, 2005	Scottrade Troy Group	Hacking	Unknown
Dec. 1, 2005	Firstrust Bank	Stolen laptop	100,000

Source: Compiled by Privacy Rights Clearinghouse (www.privacyrights.org).

CORPORATION COMMENTS

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

DATE: July 19, 2006

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

FROM: Sandra L. Thompson [Electronically produced version; original signed by Sandra L. Thompson]
Acting Director

CONCUR: John F. Bovenzi [Electronically produced version; original signed by John F. Bovenzi]
Deputy to the Chairman and Chief Operating Officer

SUBJECT: Draft Report Entitled:
FDIC's Oversight of Technology Service Providers (2005-046)

This memorandum represents the Division of Supervision and Consumer Protection (DSC) response to the draft report entitled, *FDIC's Oversight of Technology Service Providers (2005-046)* prepared by the FDIC's Office of Inspector General (OIG). The stated objective of the OIG audit was to determine the FDIC's examination coverage of technology service providers (TSPs) and related efforts to protect sensitive customer information in response to various reported security breaches in the financial industry in 2005. Specifically, this audit assessed the FDIC's oversight process for identifying and monitoring TSPs used by FDIC-supervised institutions and for prioritizing examination coverage.

The FDIC has long recognized that the protection of sensitive customer information either at financial institutions or service providers is a significant consumer protection and safety and soundness risk area. The FDIC's commitment to the protection of customer information is demonstrated by our proactive approach to enforcing data security regulations and guidance and by our overall identity theft strategy. The OIG audit contains several findings and six recommendations. As discussed below, DSC has already implemented or considered many of the recommendations. DSC also agrees with the remaining recommendations and will work with our interagency partners to enhance our supervisory programs.

OVERVIEW

To address the specialized nature of technology related supervision, risks, and controls in the banking industry, the FDIC regularly and routinely evaluates all of its regulated financial institutions' information security programs through our information technology (IT) supervision program, as well as enforcing legal privacy requirements through our compliance examination program. The FDIC also conducts IT examinations of major TSPs that support financial institutions. IT examinations of financial institutions are most often conducted by the FDIC in conjunction with safety and soundness examinations under authority granted by the FDI Act and

the Gramm Leach Bliley Act (GLBA) while IT examinations of TSPs are conducted under authority granted by the Bank Service Company Act (BSCA), usually on an interagency basis.

IT examinations of both financial institutions and TSPs are conducted to ensure the continued safe and sound operation of the financial institution(s) including the protection of customer information. IT examination procedures for both financial institutions and TSPs review IT infrastructure, processes, security, and management oversight to assess control over the confidentiality, integrity, and availability of sensitive, material, and critical bank and customer information.

IT Supervision Program

The FDIC, as part of its comprehensive IT supervision program, conducts examinations, develops industry and examiner guidance, trains examiners, develops and coordinates outreach, and conducts research related to information security and identity theft to ensure and promote information security across the industry.

IT examinations are performed in banks as part of regularly scheduled safety and soundness examinations to ensure adequate confidentiality, integrity, and availability of bank systems and to determine compliance with GLBA customer information security standards. Although the FDIC has authority under GLBA to enforce the customer information security standards in the banks it regulates, the Federal Trade Commission (FTC) has enforcement authority for any TSPs that are covered by GLBA, including those that may be examined by the FDIC under the BSCA. The FDIC ensures that banks enforce GLBA standards on the TSPs they contract with. IT examinations include assessments of the bank's oversight of TSPs through the bank's vendor management process.

The FDIC, in partnership with other Federal banking agencies, has a well defined program to identify, risk rank, and examine information security in the TSPs that pose a risk to financial institutions. The FDIC has examined data security controls in TSPs since the enactment of the BSCA in 1962. The BSCA gives Federal banking agencies broad examination authority over a variety of organizations which perform permissible bank services for a bank by contract or otherwise. While permissible bank services are described in the BSCA, the listing is not intended to be exhaustive. The FDIC and other agencies currently use the BSCA to examine a variety of technology services such as Internet banking, web hosting, imaging and e-safekeeping, ATM processing, electronic bill pay, and credit card processing. The FDIC, and other members of the Federal Financial Institutions Examination Council (FFIEC), jointly administers IT examinations of all systemically significant TSPs through its IT Subcommittee and the guidance established in the FFIEC IT Examination Handbooks.

The FFIEC IT Subcommittee directly administers the examination process for the most significant TSPs in a national TSP examination program called Multiregional Data Processing Servicers (MDPS) examinations. Currently there are 17 TSPs in the national MDPS program administered by the FFIEC. These TSPs have multiple examination activities through out the cycle at different facilities resulting in 110 separate examination activities in the 2005/2006

examination cycle. The FDIC is serving as Agency-in-Charge for 58 of those examinations. The IT Subcommittee meets at least monthly to discuss relevant issues related to the examination process and issues related to TSPs. A monthly MDPS tracking report is updated and monitored by the FFIEC.

In addition to the national MDPS program, each FFIEC member agency conducts regional TSP examinations administered at the regional level. Many of these examinations are also conducted on an interagency basis. The regional representatives for each agency meet regularly to identify and schedule regional TSP examinations. A global list of all the regional TSP examinations is updated on an annual basis in the 1st quarter of the year and shared among agencies at a national level. Currently, the FDIC is serving as Agency-in-Charge of over 77 regional TSP examinations and participating in many more led by other agencies.

Agency-in-Charge	MDPS Examinations	Regional TSP
FDIC	58	77
FRB	11	14
OCC	15	30
OTS	26	13

2005/2006 Interagency Examination Schedule. Note: the 17 TSPs in the MDPS program have multiple examination activities through out the cycle at different facilities.

Examiner Guidance

The standards and guidelines for the national and regional TSP examinations are determined on an interagency basis and published in the FFIEC IT Examination Handbooks. This guidance is updated on a two year cycle to identify new examination and risk identification techniques. For example, in February 2006, the FFIEC issued an updated Examination Priority Ranking Sheet (EPRS) as part of the new Risk-Based Examination Priority Ranking Program (RB-EPRP).

MDPS and regional TSP reports of examination are shared with other agencies in accordance with standards and procedures outlined in the FFIEC IT Examination Handbooks. Each agency stores and tracks the results of examinations. The FDIC's centralized database called the Virtual Supervisory Information on the Net (ViSION) is used to store examination information.

The standards and guidelines for conducting IT examinations of financial institutions are published in the FDIC's Information Technology Risk Management Program (IT-RMP). IT-RMP is a risk-based examination process which incorporates a variety of optional work programs such as the IT General Workprogram. These work programs address a variety of information security issues including GLBA and the notification requirements of the BSCA (section 7(c)(2)).

Industry Guidance

In addition to the joint FFIEC IT Examination Handbooks, the FDIC has issued a wide variety of guidance to the industry related to information security or preventing identity theft. In the last five years the FDIC has issued guidance on foreign and domestic outsourcing, authentication, spyware, phishing, pharming, customer response programs, disposal of customer information, software due diligence, instant messaging, patch management, pre-text calling, and more.

DSC also develops and coordinates outreach events and conducts research on identity theft and data security issues beneficial to the banking industry and consumers. As a result of recent FDIC studies regarding identity theft, the FDIC effected interagency guidance, in October 2005, requiring financial institutions and their TSPs to improve authentication methods for high-risk transactions that could result in identity theft, or allow fraud resulting from credential theft.

OIG FINDINGS, RECOMMENDATIONS AND DSC RESPONSES

Finding A: Inventory of TSPs

The OIG draft report concluded that:

> DSC does not have a current, accurate, and complete inventory of TSPs that are used by FDIC-supervised institutions and have access to sensitive customer information. Instead, the inventory is largely limited to those TSPs that are subject to separate examinations under FFIEC guidelines. In addition, TSP-related data, including data related to TSP processing of sensitive customer information, needed to perform thorough risk assessments and make fully informed decisions on examination priorities is not readily available for use in support of the TSP examination process. The primary causes of this condition are (1) outdated guidance to institutions on BSCA compliance, (2) no formal requirement for examiners to assess the adequacy of institution compliance with BSCA notification requirements, and (3) weaknesses in controls for obtaining and maintaining TSP data in the ViSION system from both BSCA notifications and IT examinations.

DSC agrees that improvements should be made. DSC relies upon its well-proven on-site IT examinations of financial institutions as the primary method for identifying a bank's TSP relationships. On-site examiners review the bank's vendor management process and identify relationships with TSPs. Examiners currently enter this information in the FDIC's centralized ViSION database. Our experience has shown that examination data derived from on-site examiner assessment is more complete and reliable than secondary forms of reported data.

The OIG report identified data integrity issues with ViSION. DSC recognizes that data integrity issues did occur as a result of an extensive multipart upgrade and conversion from the FDIC's outmoded legacy system to ViSION carried out in March 2005. Immediately thereafter, DSC

implemented a data correction process. The ViSION database listing of TSPs was substantially corrected by the end of 2005 and DSC has a high level of confidence in the current database.

In addition to examination results, DSC utilizes BSCA notifications to ensure that it identifies those TSPs which may impact financial institutions and their customers. These notifications were established under the 1962 BSCA, which requires a financial institution to give its primary federal regulator notice of the existence of TSP relationships "within 30 days of the making of the contract or the performance of the service, whichever comes first." The content and decentralized reporting process for the notifications, as determined by the BSCA, does not correspond well to the advanced technology services and relationships that FDIC examiners encounter today. Thus, DSC considers the notifications to be a less reliable source for identifying TSP relationships. DSC agrees that centralized tracking of these notices would be beneficial. To that end, DSC has created an interim stand-alone database to centralize BSCA notice results. As discussed below, DSC continues its efforts to implement a system that integrates this database with FDIC's ViSION database and will discontinue the interim database upon completion.

OIG Recommendations Regarding Finding A and DSC Responses

1) **Assess, in conjunction with the other federal banking agencies, regulatory and other options for establishing and maintaining a current, accurate, and complete inventory of TSP information through the use of BSCA notifications, examination results, and other available data. Consideration should be given specifically to the content of BSCA notifications, the initiation and termination of TSP relationships, third-party reviews and other oversight of TSPs, and the processing of sensitive customer information.**

DSC agrees that the FDIC would benefit from enhancing the centralized collection of TSP data and has already taken steps to improve the centralized collection of TSP data on both an inter-agency basis and internally. DSC will assess its options for improving the accuracy and completeness of our inventory of TSP information and will vet the issues raised in this recommendation with the other FFIEC agencies. This action will be completed by March 30, 2007.

2) **Revise IT examination guidance to address coverage of financial institution compliance with BSCA notification requirements.**

DSC agrees that IT examination procedures should include an option for a compliance review of BSCA notifications and already has included such a review in the IT General Workprogram. As indicated in our response to OIG recommendation number 4 below, DSC will review the IT Officer's Questionnaire for appropriate inclusion of BSCA notification requirements. This action will be completed and enhanced guidance will be issued by March 30, 2007.

3) **Establish policy and procedures for updating ViSION with information from BSCA notifications and the results of IT examinations, and discontinue use of a separate database for tracking these notifications.**

DSC agrees with this recommendation as it reflects current system development plans. The separate database is an interim solution until the data can be incorporated into the ViSION database. DSC will propose to the appropriate FDIC committees that the FDIC develop a centralized collection system to add BSCA notifications to the ViSION architecture. DSC will complete this action by March 30, 2007.

4) **Establish controls as part of DSC's implementation of the FDIC Data Stewardship Program to ensure the reliability and usefulness of TSP data in ViSION. Consideration should specifically be given to:**

   - **Modifying the Technology Profile Script, Officer's Questionnaire, and IT ViSION Template to identify all TSPs used by a financial institution and the relevant risk factors, including those that process sensitive customer information and third-party review results.**

DSC agrees with the intent of this recommendation and has identified a preferred alternative. The purpose of the Technology Profile Script is to identify the complexity of technology wholly within the financial institution for the purpose of assigning an appropriate skilled examiner to examine the data center within the financial institution. Thus, DSC does not believe that modifying this specific Technology Profile Script form is the best solution for identifying risks within a TSP and ensuring data reliability.

As an alternative action, DSC will review the IT Officer's Questionnaire and include a self assessment item for BSCA notification requirements where appropriate. This action will be completed by March 30, 2007. Additionally, as risk ranking methods for TSPs are determined on an interagency basis; DSC will evaluate and consider additional risk ranking measures for TSPs and will propose any relevant findings to the FFIEC IT Subcommittee for consideration. This action will also be completed by March 30, 2007.

   - **Validating, as part of the supervisory process, TSP information in the ViSION IT Examination Module.**

DSC agrees that data integrity is important and has already completed a data integrity validation process as part of its system conversion process which eliminated many of the errors noted in the draft report. DSC will review our current TSP controls and consider the opportunity for further enhancement. If enhancements are needed they will be implemented to ensure the continued data integrity of ViSION data. These actions will be completed by March 30, 2007.

   - **Enhancing the ViSION report retrieval process to allow for the retrieval of information by TSP, to include data on all financial institutions serviced, as well as by institution, to include all TSPs used.**

DSC evaluated this recommendation and determined that the ViSION database currently allows the report generating function as described by the OIG. ViSION capability currently includes the ability to report all TSPs for a given institution and all institutions serviced by a given TSP. No DSC action is warranted given that the recommended data retrieval process is available and functioning properly.

Finding B: Obtaining and Completing Examination Priority Ranking System (EPRS) Information

The OIG draft report concluded in part that:

> The FDIC's participation in the risk-based supervisory process of TSPs used by the federal banking agencies could be improved. The FDIC was not always obtaining and completing EPRS information used in scheduling and prioritizing TSP examinations in accordance with FFIEC guidance. In addition, FDIC guidance does not address the agencies' consideration of the TSPs' processing of sensitive customer information when ranking TSPs as part of the EPRS process. As a result, FFIEC decisions and FDIC input into those decisions on the risks posed by TSPs and the frequency and extent of TSP examinations could lack sufficient support.

The OIG's observations were based upon sampling results that were derived from the interagency pilot program that covered EPRS information processes. Under the pilot program the EPRS was not a mandatory part of the Report of Examination. After sufficient testing, a new Risk Based-Examination Priority Ranking Program (RB-EPRP) was adopted by the FFIEC and made permanent through the issuance of an FFIEC memorandum dated February 13, 2006. The program was officially distributed to FDIC examiners through DSC RD Memorandum 06-013 published on May 1, 2006. The provisions of the program now extend to all TSPs and the ranking form, previously called the EPRS, will be the first two pages of the confidential section of the TSP Report of Examination. The TSP IT Handbook is currently being rewritten, by the FFIEC to include the new procedures. As a result, supervisory decisions based upon this data now have sufficient support.

OIG Recommendations Regarding Finding B and DSC Responses

5) Issue supplemental guidance to the TSP Handbook on the completion and sharing of EPRSs among the federal banking agencies and the consideration of TSPs' processing of sensitive customer information in assigning risk factors to the TSPs.

As described above, supplemental guidance has been issued by the FFIEC and the FDIC. Additionally, FDIC will raise the topic of including "sensitive customer information" in the risk ranking method to the FFIEC IT Subcommittee for discussion and consideration. This action will be completed by September 30, 2006.

6) **Assess the merits of implementing an automated process, including the use of ViSION, for collecting, storing, monitoring, and sharing EPRSs and other TSP-related information with the other federal banking agencies comprising the FFIEC.**

The FFIEC is currently reviewing the technical feasibility of adopting a system for entering and sharing RB-EPRP form data between agencies. DSC will forward this OIG recommendation to the FFIEC IT Subcommittee for interagency review and consideration. DSC will complete this action by September 30, 2006.

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. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	DSC will assess its options for improving the accuracy and completeness of the TSP inventory information and will vet the issues with the other FFIEC agencies.	March 30, 2007	N/A	Yes	Open
2	DSC will review the IT Officer's Questionnaire for appropriate inclusion of BSCA notification requirements.	March 30, 2007	N/A	Yes	Open
3	DSC will propose to the appropriate FDIC committees that the FDIC develop a centralized collection system to add BSCA notifications to the ViSION architecture.	March 30, 2007	N/A	Yes	Open
4	DSC will review the IT Officer's Questionnaire and include a self-assessment item for BSCA notification requirements where appropriate. Additionally, DSC will evaluate and consider additional risk-ranking measures for TSPs and will propose any relevant findings to the FFIEC IT Subcommittee for consideration. Also, DSC will review current TSP controls and consider the opportunity for further enhancement.	March 30, 2007	N/A	Yes	Open
5	Supplemental guidance has been issued by the FFIEC and the FDIC. DSC will raise the topic of including sensitive customer information in the risk-ranking method to the FFIEC IT Subcommittee for discussion and consideration in the risk-based examination priority ranking program.	September 30, 2006	N/A	Yes	Open
6	DSC will raise the issue of TSP processing of sensitive customer information with the FFIEC IT Subcommittee for interagency review and consideration.	September 30, 2006	N/A	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.