

FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL

Semiannual Report to the **Congress**



★ ★ ★ ★ ★ **October 1, 2006 – March 31, 2007** ★ ★ ★ ★ ★





The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 4,540 individuals within seven specialized operating divisions and other offices carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured \$6.64 trillion in deposits for 8,693 institutions, of which the FDIC supervised 5,220. The Corporation held insurance funds of \$50 billion to ensure depositors are safeguarded.

FEDERAL DEPOSIT INSURANCE CORPORATION
OFFICE OF INSPECTOR GENERAL

Semiannual Report to the **Congress**



★ ★ ★ ★ ★ **October 1, 2006 – March 31, 2007** ★





Inspector General's Statement

★ ★ ★ ★ ★ ★ ★ ★ ★ ★

M

My office continues to achieve significant results as we carry out the Office of Inspector General (OIG) mission at the Federal Deposit Insurance Corporation (FDIC) through audits, evaluations, investigations, and other operational activities. Over the past 6 months, we issued 11 audit and evaluation reports with 35 nonmonetary recommendations to management for enhancements in such areas as the FDIC's supervision of financial institutions' Office of Foreign Assets Control compliance programs, implementation of the 2005 amendments to the Community Reinvestment Act regulations, protection of information in an identifiable form, information technology examination coverage of financial institutions' oversight of technology service providers, and the FDIC's contract planning and management for business continuity.

As discussed in more detail in our report, we also closed 30 criminal investigations, and our investigations resulted in over \$75 million in total fines, restitution, and other potential monetary recoveries. Of great significance, during the reporting period, at the conclusion of one of the OIG's most successful investigations, in the U.S. District Court for the Southern

District of Florida, a restitution order in the aggregate amount of \$31.7 million was issued. The former Hamilton Bank chairman of the board and chief executive officer (CEO) was ordered individually to pay a total of \$16.1 million to the FDIC, and \$1.1 million to Twin City Fire Insurance Company. These amounts represent restitution of losses suffered as a result of the bank fraud for which the former chairman of the board and CEO was convicted in May 2006. As a result of the securities fraud for which he was convicted, the former chairman of the board and CEO was also ordered to pay \$14.5 million in restitution, jointly and severally, with his two co-defendants, the former Hamilton president and the former chief financial officer.

The OIG is especially proud of Special Agent Gary Sherrill, from our Atlanta Office, whose investigative efforts were instrumental in the successful outcome of the Hamilton case. Gary's outstanding work will be acknowledged by FDIC Chairman Sheila Bair at the Corporation's annual award ceremony in early May when he will receive the Chairman's Award for Excellence for his individual efforts in this case. We are honored by the Chairman's recognition of

Gary's investigation of a highly complex financial institution fraud and his efforts to ensure the nation's banks operate safely and soundly.

During the reporting period, I selected Sara Gibson to serve as Assistant Inspector General for Investigations. I also announced a reorganization of the OIG to include an Office of Evaluations that would be separate from our Office of Audits. The Evaluations group, led by Stephen Beard, Assistant Inspector General for Evaluations and Management, is undertaking a number of assignments designed to provide independent, objective information to facilitate FDIC management decision-making and improve operations. The group has already completed several successful engagements. We have also continued implementing a number of internal OIG initiatives to build and sustain a high-quality OIG work environment. In that connection, over the past 6 months we have initiated many projects to promote professional training and development of our staff. We have also engaged in a number of stakeholder outreach efforts to maintain mutually beneficial working relationships with the Congress, corporate officials, others in the

Inspector General community, and the Government Accountability Office. These activities are proving highly beneficial and will continue as we plan for 2008 and 2009.

I am especially grateful to FDIC Chairman Bair for her support of my office over the past months. Similarly, FDIC Vice Chairman Gruenberg, who also chairs the FDIC Audit Committee, continues to endorse the role of the FDIC OIG, as evidenced by his recent remarks at our OIG-wide conference in April.

In closing, I underscore the theme of that recent OIG conference—Change, Challenge, Choices. The OIG has experienced significant changes over the past months and, like everyone at the FDIC, is attuned to changes and emerging risks in the financial services industry and the regulatory arena everyday. These changes pose challenges to us all. Our choice is and will continue to be to approach the challenges with a positive attitude of service to the Corporation and the public interest. We are honored to do so.

Jon T. Rymer
Inspector General
April 30, 2007

Table of Contents



| | |
|--|----|
| Inspector General’s Statement..... | 3 |
| Highlights and Outcomes | 7 |
| Strategic Goal Areas | |
| Supervision: Assist the FDIC to Ensure the Nation’s Banks Operate Safely and Soundly | 11 |
| Insurance: Help the FDIC Maintain the Viability of the Insurance Fund | 31 |
| Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy..... | 33 |
| Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships | 39 |
| Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, Information Technology, and Physical Resources.... | 43 |
| OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment | 51 |
| Reporting Requirements | 58 |
| Information Required by the Inspector General Act of 1978, as amended | 59 |
| Abbreviations and Acronyms | 6 |

Abbreviations and Acronyms

| | |
|---------------|---|
| BCP | Business Continuity Plan |
| BSA | Bank Secrecy Act |
| CEO | chief executive officer |
| CRA | Community Reinvestment Act |
| DIT | Division of Information Technology |
| DRR | Division of Resolutions and Receiverships |
| DSC | Division of Supervision and Consumer Protection |
| ECU | Electronic Crimes Unit |
| FBI | Federal Bureau of Investigation |
| FDIC | Federal Deposit Insurance Corporation |
| FEDSIM | Federal Systems Integration Management Center |
| GSA | General Services Administration |
| IIF | information in an identifiable form |
| ILC | industrial loan company |
| ISB | intermediate small bank |
| ISC | infrastructure services contract |
| IT | Information Technology |
| IT-RMP | Information Technology-Risk Management Program |
| OA | Office of Audits |
| OCC | Office of the Comptroller of the Currency |
| OE | Office of Evaluations |
| OERM | Office of Enterprise Risk Management |
| OFAC | Office of Foreign Assets Control |
| OI | Office of Investigations |
| OIG | Office of Inspector General |
| PCIE | President's Council on Integrity and Efficiency |
| SRA | SRA International, Inc. |
| TSP | technology service provider |

Highlights and Outcomes



The OIG's 2007 Business Plan contains five strategic goals that are closely linked to the FDIC's mission, programs, and activities, and one that focuses on the OIG's internal business and management processes. These highlights show our progress in meeting these goals during the reporting period. A more in-depth discussion of OIG audits, evaluations, investigations, and other activities in pursuit of these goals follows.

Strategic Goal 1 **Supervision: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly**

Our work in helping to ensure that the nation's banks operate safely and soundly takes the form of audits, investigations, evaluations, and extensive communication and coordination with FDIC divisions and offices, law enforcement agencies, other financial regulatory OIGs, and banking industry officials. During the reporting period, in audit reports issued, we made recommendations to enhance protection from risks associated with e-banking, ensure that examinations adequately consider the reliability of appraisals and sufficiency of insurance coverage when evaluating an institution's lending activities, and

strengthen the supervisory approach for ensuring financial institution compliance with Office of Foreign Assets Control compliance programs.

With respect to investigative work, as a result of cooperative efforts with U.S. Attorneys throughout the country, numerous individuals were prosecuted for financial institution fraud, and we achieved successful results in combating a number of emerging mortgage fraud schemes. Particularly noteworthy results include a restitution order in the aggregate amount of \$31.7 million that was issued in connection with our investigation of Hamilton Bank and bank fraud on the part of former bank officers. The restitution was ordered on the former chairman of the board and chief executive officer, and his co-defendants, the former president and the former chief financial officer of the failed bank. In another significant case, in the U.S. District Court for the District of Colorado, the former BestBank owner and chief executive officer and chairman of the board of directors, the former president and director, and the former chief financial officer were found guilty of 15 felony counts of fraud and conspiracy related to BestBank's \$248 million failure in 1998. (See pages 11-30.)



Strategic Goal 2

Insurance: Help the FDIC Maintain the Viability of the Insurance Fund

Ongoing audit work related to the FDIC's dedicated examiner program will help ensure that the Corporation's Dedicated Examiner Program is contributing to the FDIC's efforts to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund. Given that the FDIC is not generally the primary federal regulator for the largest financial institutions, this program has placed dedicated examiners in the six largest insured depository institutions to work in cooperation with primary supervisors and bank personnel to obtain real-time access to information about the risk and trends in those institutions. (See pages 31-32.)

Strategic Goal 3

Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

Audits and investigations contributed to the FDIC's protection of consumers in several ways. We issued a report on information technology (IT) examination coverage

of financial institutions' oversight of technology service providers and made recommendations to help in protecting customers from identity theft and institutions from fraud and reputational and other risks associated with unauthorized access to or use of customer information. As a result of audit work related to amendments to Community Reinvestment Act regulations, we suggested strengthened examiner guidance for implementing and reporting on community development tests and development of a strategy for measuring the impact of amendments to the regulations. From an investigative standpoint, our Electronic Crimes Unit responded to phishing schemes where the FDIC and OIG Web sites were misused to entice consumers to divulge personal information and successfully shut down several Web sites used for such purposes. The Electronic Crimes Unit was also successful in deactivating Web sites and/or fax numbers involving fraudulent claims of FDIC insurance or affiliation. (See pages 33-38.)

Strategic Goal 4

Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

We gained a better understanding of the implications of a large bank failure through monitoring of a large bank resolution scenario. We also began an assignment to evaluate the design and implementation of selected controls established by the Division of Resolutions and Receiverships to safeguard sensitive information collected and maintained in electronic form in resolution and receivership activities at FDIC-insured institutions. We continued to pursue concealment of assets investigations related to the more than \$1.7 billion in criminal restitution that the FDIC is owed. In connection with one such case worked in conjunction with the FDIC Legal Division, during the reporting period the former chief executive officer of Sunbelt Savings and Loan, Dallas, Texas, was sentenced to 97 months of incarceration and ordered to pay a criminal forfeiture of more than \$2 million to the U.S. government and restitution of more than \$300,000 to the FDIC. (See pages 39-42.)

Strategic Goal 5

Resources Management: Promote Sound Governance and Effective Stewardship and Security of Human, Financial, IT, and Physical Resources

We issued several audit and evaluation reports in this goal area and made recommendations to strengthen contract planning and management for business continuity, ensure appropriate use of information in an identifiable form and enhanced protection of sensitive FDIC data, strengthen contract administration and oversight of IT support services for the Corporation, and improve information security controls. We reported on the FDIC's succession planning efforts. We also promote integrity in FDIC internal operations through ongoing OIG Hotline referrals, investigations of employee cases, and coordination with the FDIC's Ethics Office. (See pages 43-50.)

Strategic Goal 6

OIG Internal Processes: Build and Sustain a High-Quality OIG Work Environment

We focused increased attention on a number of activities in this goal area during the past 6 months. We

encouraged individual growth through professional development by way of initiatives such as training and development and career development plans for OIG staff and expanding the OIG mentoring program. We also strengthened human capital management and leadership development by developing end-of-assignment feedback mechanisms for staff, incorporating leadership training in training and development plans, and updating the OIG's business continuity and emergency preparedness plans and procedures. Our office continued to foster positive stakeholder relationships by way of OIG executives meetings with FDIC executives; presentations at Audit Committee meetings; congressional interaction; coordination with financial regulatory OIGs, other members of the Inspector General community, other law enforcement officials, and the Government Accountability Office. New members of the OIG Employee Advisory Group took office, and we maintained and updated the OIG Web site to provide easily accessible information to parties interested in our office and the results of our work.

We conducted internal quality reviews of Office of Audits assignments and various Office of Investigations operational components and began work to revise audit policies and procedures to address changes in the 2007 revision to Government Auditing Standards, process changes resulting from an internal assignment management review, and external peer review results. To ensure cost-

| Significant Outcomes (October 2006 - March 2007) | |
|--|---------------------|
| Audit and Evaluation Reports Issued | 11 |
| Nonmonetary Recommendations | 35 |
| Investigations Opened | 32 |
| Investigations Closed | 30 |
| OIG Subpoenas Issued | 25 |
| Judicial Actions: | |
| Indictments/Informations | 18 |
| Convictions | 26 |
| OIG Investigations Resulted in: | |
| Fines of | \$675 |
| Restitution of | \$70,062,511 |
| Asset Forfeiture of | \$5,500,000 |
| Total | \$75,563,186 |
| Cases Referred to the Department of Justice (U.S. Attorney) | 27 |
| Cases Referred to FDIC Management | 2 |
| OIG Cases Conducted Jointly with Other Agencies | 111 |
| Hotline Allegations Referred | 79 |
| Proposed Regulations and Legislation Reviewed | 3 |
| Proposed FDIC Policies Reviewed | 21 |
| Responses to Requests and Appeals under the Freedom of Information Act | 4 |

effective and secure IT, we continued to coordinate closely with the FDIC's Division of Information Technology. We are also taking steps to identify and evaluate options and requirements needed to streamline, enhance, and improve collection and reporting of information to manage OIG audits and evaluations. We implemented upgrades to the OIG's training system and updated the OIG's internal Business Plan 2007 Dashboard to capture progress on achievement of strategic and performance goals. (See pages 51-56.)



Strategic Goal 1: **Supervision: Assist the FDIC to Ensure the Nation's Banks Operate Safely and Soundly**

Bank supervision is fundamental to the FDIC's efforts to ensure stability and public confidence in the nation's financial system. As of December 31, 2006, the FDIC was the primary federal regulator for 5,220 FDIC-insured, state-chartered institutions that were not members of the Federal Reserve System (generally referred to as "state non-member" institutions). The Department of the Treasury (the Office of the Comptroller of the Currency and the Office of Thrift Supervision) or the Federal Reserve Board supervise other banks and thrifts, depending on the institution's charter. While the number of institutions where the FDIC is the primary federal supervisor showed a steady decline over the past 4 years, the dollar value of assets held by those institutions showed a steady increase during the same period. The Corporation also has back-up examination authority to protect the interests of the deposit insurance fund for more than 3,473 (as of December 31, 2006) national banks, state-chartered banks that are members of the Federal Reserve System, and savings associations.

Another important aspect of the FDIC's supervisory responsibilities relates to industrial loan companies (ILCs). The FDIC is the primary federal

regulator for a number of ILCs, which are limited-charter depository institutions. ILCs may be owned by commercial firms, and these parents may not be subject to consolidated supervision by a federal banking regulator. As of September 30, 2006, there were 58 operating ILCs with aggregate total assets of \$177 billion. The FDIC must establish and maintain effective controls in its processes for granting insurance to, supervising, and examining ILCs, taking into consideration the relationship between the ILC and its parent company and the effect of such a relationship on the ILC. This is especially important when the ILC's parent company is not subject to the scope of consolidated supervision, consolidated capital requirements, or enforcement actions imposed on parent organizations subject to the Bank Holding Company Act.

In recent years, the banking industry has been marked by consolidation, globalization, and the development of increasingly complex investment strategies available to banks. Bank regulators, both domestically and internationally, have devised new standards for bank capital requirements commonly referred to as Basel IA and Basel II. The FDIC and the other bank regulators continue to assess



the potential impact of new standards on bank safety and soundness.

The FDIC has adopted a risk-focused approach to examining financial institutions to minimize regulatory burden and direct its resources to those areas that carry the greatest potential risk. The FDIC must also ensure that financial institutions have adequate corporate governance structures relative to the bank's size, complexity, and risk profile to prevent financial losses and maintain confidence in those entrusted with operating the institutions. The FDIC's follow-up processes must be effective to ensure institutions are promptly complying with supervisory actions that arise as a result of the FDIC's examination process.

The Corporation is also faced with developing and implementing programs to minimize the extent to which the institutions it supervises are involved in or the victims of financial crimes and other abuse. Increased reliance by both financial institutions and non-financial institution lenders on third-party brokers has also increased opportunities for increased real-estate frauds, including property flipping and other mortgage frauds. Examiners must be alert to the possibility of such fraudulent activity in financial institutions—it is purposeful and often hard to detect.

Part of the FDIC's overall responsibility and authority to examine banks for safety and soundness is the responsibility for examining state-chartered non-member financial institutions for compliance with the Bank Secrecy Act (BSA). The BSA requires financial institutions to keep records and file reports on certain financial transactions. FDIC-supervised institutions must establish and maintain procedures to assure and monitor compliance with BSA requirements. An institution's level of risk for potential money laundering determines the necessary scope of the BSA examination. In a related vein, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) promulgates, develops, and administers economic and trade sanctions such as trade embargoes, blocked assets controls, and other commercial and financial restrictions under the provisions of various laws. Generally OFAC regulations prohibit financial institutions from engaging in transactions with the governments of, or individuals or entities associated with, foreign countries against which federal law imposes economic sanctions. Sanctions can also be used against international drug traffickers, terrorists, or foreign terrorist organizations, regardless of national affiliation.



In its role as supervisor, the FDIC also analyzes data security threats, occurrences of bank security breaches, and incidents of electronic crime that involve financial institutions. Misuse and misappropriation of personal information are emerging as major developments in financial crime. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving.

The OIG's role under this strategic goal is conducting audits and evaluations that review the effectiveness of various FDIC programs and examination processes aimed at providing continued stability to the nation's banks. Another major means of achieving this goal is through investigations of fraud at FDIC-supervised institutions; fraud by bank officers, directors, or other insiders; fraud leading to the failure of an institution; fraud impacting multiple institutions; and fraud involving monetary losses that could significantly impact the institution.

To assist the FDIC to ensure the nation's banks operate safely and soundly, the OIG's 2007 performance goals are as follows:


- Protect and ensure the effectiveness and efficiency of the FDIC's Supervision Program, and
- Assist FDIC efforts to detect and prevent BSA violations, money laundering, terrorist financing, fraud, and other financial crimes in FDIC-insured institutions.

OIG Work in Support of Goal 1

The OIG's Office of Audits issued three reports in the Supervision area in furtherance of our safety and soundness-related goal during the reporting period, as discussed below.

Division of Supervision and Consumer Protection's Information Technology-Risk Management Program

Interagency guidelines require financial institutions to implement a comprehensive written information security program. To ensure that FDIC-supervised financial institutions implement adequate information security program controls, the Corporation conducts periodic onsite information technology (IT) examinations and, in August 2005, the Division of Supervision and Consumer Protection (DSC) established the Information Technology-Risk Management Program (IT-RMP). IT-RMP replaced the broad-based technology



and control reviews conducted under the former IT examination program.

During the reporting period, we conducted an audit to determine whether the FDIC has established and implemented adequate procedures for addressing IT security risks at FDIC-supervised institutions that offer electronic banking products and services. We focused this review on the IT-RMP and DSC's examiner training framework in relationship to the new program.

We reported that DSC has established procedures within the IT-RMP for addressing IT security risks at FDIC-supervised financial institutions. These procedures address most of the information security requirements contained in interagency guidance. Our review of 12 IT examinations found that examiners generally followed the procedures outlined in the IT-RMP. We also noted that improvements to the IT-RMP program would help to ensure adequate and consistent implementation of the IT-RMP and related examination procedures.

Specifically, DSC could revise certain IT-RMP tools to assist examiners in more effectively identifying relevant IT security risks to be assessed. Additionally, updated IT-RMP guidance could more clearly address the

methodology examiners should use in deriving the IT composite rating for a financial institution. Such clarified guidance would increase assurance that IT ratings accurately and consistently reflect the effectiveness of an institution's IT risk management practices and the adequacy of its information security program.

We made seven recommendations to enhance the tools and guidance under the IT-RMP methodology and the IT training programs. FDIC management generally agreed with our recommendations and is taking responsive action to review DSC's tools, guidance, and training programs as part of an evaluation of the first year of performance under the IT-RMP program.

FDIC's Supervision of Financial Institutions' Compliance with Office of Foreign Assets Control Compliance Programs

During the reporting period, we conducted an audit to determine whether the FDIC's DSC provides effective supervision of compliance with OFAC regulations by FDIC-supervised institutions.

We determined that the FDIC's supervisory approach to OFAC compliance includes examinations



of controls established and implemented by FDIC-supervised financial institutions to ensure compliance with OFAC regulations. For the examinations we reviewed, FDIC examiners generally followed interagency guidelines in assessing the appropriateness of implemented controls and whether those controls were commensurate with the financial institutions' specific product lines, customer base, nature of transactions, and identification of high-risk areas. In addition, the FDIC has taken important steps to address institutions' OFAC compliance, such as participating in developing and issuing interagency guidance for examiners and banking organizations, including notifications on updates to OFAC's Specially Designated Nationals and Blocked Entities list; conducting OFAC-related training and outreach activities for examiners and the banking industry; issuing BSA-related cease and desist orders that included OFAC-related provisions; and signing an interagency Memorandum of Understanding, which governs information-sharing between the Federal Banking Agencies and OFAC.

We noted that DSC could enhance its supervisory approach to OFAC compliance by monitoring and tracking

financial institution OFAC sanctions violations, compliance program deficiencies, and OFAC-related enforcement actions; and issuing additional guidance to examiners to ensure consistent and comprehensive documentation of OFAC compliance to better assist the FDIC and subsequent examination teams in ensuring financial institution compliance with OFAC laws and regulations. DSC management concurred with two of our four recommendations in this regard and agreed with the intent of the remaining two recommendations. Management's comments were responsive to all recommendations.

We also identified a matter for congressional consideration regarding examination and enforcement authorities associated with institution compliance with OFAC regulations. Specifically, a more comprehensive statutory and regulatory framework exists for the examination and enforcement of BSA compliance and the establishment of BSA compliance programs than for OFAC compliance, although both BSA and OFAC requirements address national security and law enforcement concerns.



Examination Assessment of the Reliability of Appraisals and Sufficiency of Insurance Coverage for Real Estate Lending

Another of our audits during the reporting period was designed to determine whether FDIC examiners adequately consider the reliability of appraisals and sufficiency of insurance coverage for collateral as part of an assessment of an institution's lending policies, procedures, and practices related to real estate loans. This audit focused primarily on institution and examination guidance.

We found that the FDIC's guidance to institutions and examiners on the reliability of appraisals and sufficiency of property and flood insurance for real estate loans was generally adequate. As for the application of existing examination guidance, based on a limited sample of 11 institutions, we found that examiners had reviewed appraisal information as part of their assessment of a financial institution's residential real estate lending and loan portfolio management. We also found that examiners had considered the sufficiency of property and flood insurance for the 11 examinations. However, for 6 of the 11 examinations we reviewed, we found limited evidence in the

examination documentation that examiners had specifically considered the reliability of appraisals as part of an institution's real estate appraisal program. As a result, there was inadequate assurance that these institutions were complying with the minimum appraisal standards in the FDIC Rules and Regulations designed to ensure the reliability of appraisals.

Overall, the examinations we reviewed adequately considered the sufficiency of property insurance and flood insurance coverage for collateral on real estate loans; however, we identified one area of concern. This area relates to ensuring that institutions have adequate controls to avoid flood insurance lapses in cases where escrowing is not performed. Both the borrowers and the institutions are exposed to a greater risk of an uninsured loss from flooding during a period of lapsed insurance.

Finally, we learned that a lapse in flood insurance coverage can occur in situations where a financial institution that is not escrowing for flood insurance premiums must purchase flood insurance because a borrower has not maintained such coverage. This lapse can occur because the required 45-day waiting period under the Flood Disaster Protection



Act—after which a financial institution is required to purchase flood insurance on behalf of the borrower—is longer than the 30-day grace period, as set forth in National Flood Insurance Program guidelines, during which insurance coverage remains in effect after expiration. Thus, the borrower and financial institution may have no flood insurance coverage for 15 days or more until the institution is able to purchase flood insurance on behalf of the borrower. We provided this information to assist the Congress in considering whether legislative action regarding flood insurance would help reduce the risk associated with flood insurance policy lapses.

Our report recommended that DSC enhance guidance related to (1) examiners ensuring the reliability of appraisals and (2) institutions addressing the need for adequate controls to avoid lapses in flood insurance coverage. DSC management concurred with the findings and recommendations.

Ongoing Audit Work

The OIG's ongoing work in this strategic goal area includes a review of the FDIC's oversight of subprime lending at FDIC-supervised institutions. Subprime lending refers to programs that target borrowers

with weakened credit histories typically characterized by payment delinquencies, previous charge-offs, judgments, or bankruptcies. Over the years, subprime lending volumes have increased significantly. In July 2001, federal banking regulatory agencies issued expanded examination guidance on subprime lending. Our approach to auditing this area is to look at subprime practices related to specific business lines, namely mortgages, credit cards, and automobile loans. Our first focus is on subprime credit card banks.

Another significant assignment in this area relates to implementation of the USA Patriot Act. We are conducting audit work to determine whether examination procedures are designed to evaluate institution compliance with the anti-money laundering and terrorist financing provisions of the Act and whether those procedures are fully and consistently implemented to provide reasonable assurance that institutions with weak programs for detecting money laundering and terrorist financing activity will be identified and appropriate corrective measures imposed.



Successful OIG Investigations Uncover Financial Institution Fraud

The OIG's Office of Investigations' work focuses largely on fraud that occurs at or impacts financial institutions. The perpetrators of such crimes can be those very individuals entrusted with governance responsibilities at the institutions—directors and bank officers. In other cases, individuals providing professional services to the banks, others working inside the bank, and customers themselves are principals in fraudulent schemes.

The following cases from the reporting period are illustrative of some of the OIG's success in pursuing strategic goal 1 during the reporting period. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, U.S. Attorneys Offices, and others in the law enforcement community.

Convicted Hamilton Bank Officers Ordered to Pay \$32 Million in Total Restitution for Bank and Securities Fraud

On October 20, 2006, in the U.S. District Court for the Southern District of Florida, a restitution order in the aggregate amount of

\$31.7 million was issued in the Hamilton Bank (Hamilton) case. The former Hamilton chairman of the board and chief executive officer was ordered individually to pay a total of \$16.1 million to the FDIC, and \$1.1 million to Twin City Fire Insurance Company (Twin City). These amounts represent restitution of losses suffered as a result of the bank fraud for which the former chairman of the board was convicted in May 2006. The restitution to Twin City will reimburse the company for money previously paid to the FDIC pursuant to a civil settlement following Hamilton's failure.

As a result of the securities fraud for which he was convicted, the former chairman of the board was also ordered to pay \$14.5 million in restitution, jointly and severally, with his two co-defendants, the former Hamilton president and the former chief financial officer.

On May 10, 2006, the former chairman of the board was convicted by a jury of all charges against him following a month-long trial in Miami, Florida. He was found guilty of each of the 10 objects of the conspiracy contained in the second superseding indictment. He was also convicted of each of the 15 substantive counts charged in the indictment.



OIG Special Agent Gary Sherrill, recipient of the FDIC Chairman's 2006 Award for Excellence, was instrumental in the successful outcome of the Hamilton Bank case.

Those charges consisted of wire fraud, bank fraud, securities fraud, obstruction of a bank examination, false statements, and obstruction of an agency proceeding. The former president pleaded guilty to two counts of securities fraud, and the former chief financial officer pleaded guilty to one count of securities fraud and one count of obstruction of a formal agency proceeding. Both men pleaded guilty before the trial and cooperated with the government during the investigation.

On July 26, 2006, the former chairman of the board was sentenced to a total of 30 years of incarceration and 36 months of supervised release. The former president and chief financial officer were each sentenced to serve 28 months in prison, to be followed by 24 months of supervised release.

The defendants participated in a fraudulent scheme whereby they falsely inflated the results of operations, earnings, and financial condition of Hamilton Bancorp in the Securities and Exchange Commission filings; obstructed the Office of the Comptroller of the Currency's (OCC) examination of Hamilton Bank; and lied to the investing public, the bank and securities regulators, and

their accountants regarding the true financial health of Hamilton Bancorp and Hamilton Bank. In 1998 and 1999, the three defendants engaged in swap transactions (or "adjusted price trades") to hide Hamilton Bank's losses on certain loans, including more than \$22 million in losses in 1998, and falsely accounted for the transactions to make it appear that no losses had been incurred. While the defendants falsely reported the nature of the swap transactions to the investing public and the regulators, the indictment cited recorded conversations in which the defendants openly discussed the transactions as swaps. During 1998, Hamilton Bancorp had a market capitalization of more than \$300 million.

Hamilton Bank was South Florida's highest profile trade finance bank before it ran into trouble with its regulator, the OCC, over a number of issues, including the questionable loan swaps that allowed the bank to hide \$22 million in losses in 1998. The OCC closed the bank in January 2002, and the FDIC took on liquidation responsibilities as receiver.

Investigation conducted by the FDIC OIG; prosecuted by the U.S. Attorney's Office for the Southern District of Florida.



Judge Convicts Former BestBank Executives of Fraud Related to 1998 BestBank Failure

On February 12, 2007, in the U.S. District Court for the District of Colorado, the former BestBank owner and chief executive officer and chairman of the board of directors, the former president and director, and the former chief financial officer, were found guilty of 15 felony counts of fraud and conspiracy relating to BestBank's \$248 million failure in 1998.

After a 3-week trial in August 2005, other co-defendants—the owners of Century Financial Services, Inc. and its successor Century Financial Group, Inc., were found guilty by a federal jury on charges of bank fraud, wire fraud, filing false bank reports, and continuing a financial crimes enterprise in connection with the 1998 failure of BestBank.

From 1994 through July 1998, all of these defendants jointly engaged in a business operation that made more than 500,000 BestBank credit card loans to subprime borrowers. Subprime credit card borrowers are high-risk borrowers with poor credit histories. The credit card accounts were funded by BestBank using money from depositors. BestBank attracted depositors by offering above-

market interest rates. In July 1998, the bank was closed. The Colorado State Banking Commissioner and the FDIC determined that the value of the subprime credit card loans maintained as an asset on the books of BestBank was overstated because delinquent loans were fraudulently made to appear non-delinquent. BestBank's liability to its depositors exceeded the value of its other assets, making it insolvent and one of the largest bank failures.

BestBank entered into agreements with Century Financial to market the BestBank credit cards to subprime borrowers. Century Financial sold \$498 travel club memberships, marketed first through Universal Tour Travel Club and later through All Around Travel Club. In almost every instance, those who signed up for the travel club did not pay cash for their membership. Instead, BestBank and Century Financial offered to finance a travel club membership for sub-prime borrowers using a newly issued BestBank VISA credit card. The credit limit for the subprime borrowers as provided by the bank was \$600. BestBank also charged fees, which immediately brought the borrowers close to the credit limit. Less than half of those



who signed up for the travel club received their membership materials.

The defendants carried out a fraudulent scheme in several ways. Most people did not pay the mandatory \$20 service fee required before the account was funded. Over 50 percent of the sub-prime borrowers' accounts were non-performing.

BestBank and Century Financial, in many instances, did not send the sub-prime borrowers their credit card or monthly statements. The two owners of Century Financial fraudulently concealed the sub-prime borrowers' non-performance and delinquency rates by reporting non-performing accounts as performing. The Century owners paid \$20 to some accounts so they would appear to be performing when, in fact, they were not.

BestBank was an FDIC-regulated institution that was closed on July 23, 1998, by the Colorado State Banking Commission and the FDIC, making it one of the largest bank failures in the United States in the last 10 years. Depositors' losses exceeded \$200 million. The FDIC's Bank Insurance Fund covered all depositors' losses except for \$27 million of deposits which exceeded the \$100,000 per-account insurance limit.


Joint investigation by the FDIC OIG, the Federal Bureau of Investigation (FBI), and the Internal Revenue Service Criminal Investigative Division; prosecuted by the U.S. Attorney's Office for the District of Colorado.

Former Exchange Bank President Indicted on 13 Counts of Bank Fraud

On December 12, 2006, the former president of Exchange Bank, Gibbon, Nebraska, was indicted on eight counts of bank fraud, four counts of making false bank entries, and one count of making a false statement to the FDIC. Exchange Bank lost approximately \$1 million due to the alleged fraudulent activities of the defendant.

The indictment alleges that from July 2001 through June 2004, the former president entered into loan agreements and loaned money from the bank to individuals for the purpose of inflating his loan portfolio with Exchange Bank. When the loans were not paid off, the former president would take the money out of third parties' accounts with the bank without the account holders' knowledge in order to make payments on suspect creditors' loans and would then falsify documents to cover up the illegal transactions.

In addition, the defendant allegedly directed individuals to provide false vehicle inventories and real estate



information to falsely represent collateral for questionable loans. He allegedly signed and approved the false financial documents, which gave the impression that collateral was available for the loan in question, when in fact, the collateral stated did not exist and the financial documents were materially false and inflated. When the defendant received cash payments from individuals with questionable loans, he would not apply those cash transactions to loan payments but kept those payments for his own use.

The indictment also alleges that the defendant provided cashier's checks to third parties and would falsify or fail to provide proper documentation for the entry of the cashier's check. These checks would then be provided to third parties for the benefit of both the former bank president and the third party, without proper funds to support the transaction, thereby causing a loss to Exchange Bank.

Joint investigation by the FDIC OIG and the FBI, based on a referral from DSC; prosecuted by the U.S. Attorney's Office for the District of Nebraska.

Former President and CEO of Farmers Deposit Bank Charged in a 30-Count Indictment

On December 7, 2006, the former president and CEO of Farmers Deposit Bank, Eminence, Kentucky, was charged in the U.S. District Court for the Eastern District of Kentucky, with 29 counts of bank fraud and one count of misapplication of bank funds.

The indictment charged that the defendant concealed substantial losses to the bank by various methods, including making loans under false or misleading names to nominee borrowers in an effort to keep other loans current. The defendant was also charged with altering documents (or causing documents to be altered) that were presented to the Farmers' Board of Directors, altering loan documents to postpone due dates, and structuring loans to avoid detection by the bank's Board of Directors. The indictment also charged that the defendant misapplied the proceeds of a loan and released solvent borrowers from their loan obligations before the obligations were satisfied.

Joint investigation by the FDIC OIG and the FBI based upon a referral from the FDIC Legal Division and DSC; prosecution is being handled by the U.S. Attorney's Office for the Eastern District of Kentucky.



Former President of Canton State Bank and His Wife Plead Guilty to Bank Fraud and False Statements

On February 8, 2007, in the U.S. District Court for the Eastern District of Missouri, the former president of Canton State Bank and his wife pleaded guilty to fraud charges involving false statements to obtain loans and nominee loans. As previously reported, the defendants were charged in a 26-count indictment in June 2006.

The indictment charged that between October 2001 and August 2004, the defendants understated their liabilities on loan applications with Canton State Bank, The Paris National Bank, Perry State Bank, Bank of Monticello, and the Farm Service Agency. In addition, the defendants represented to Perry State Bank and the Farm Service Agency that the livestock and farm equipment that they pledged as collateral security for loans was free and clear of all other liens and encumbrances, when they had previously pledged the same collateral for other loans.

Further, between August 2002 and May 2003, the former president allegedly made numerous loans to a bank customer, who then wrote checks to return a substantial portion


of the loan proceeds to the former president. In some cases, the payee on those checks was listed as the former president's wife's minor child in order to conceal the payments to him.

As part of his plea agreement, the former president also stipulated to an action under 8(e) of the Federal Deposit Insurance Act, which provides for a lifetime ban from banking.

Joint investigation by the FDIC OIG, the FBI, and the U.S. Department of Agriculture OIG, based on a referral from DSC; prosecuted by the U.S. Attorney's Office for the Eastern District of Missouri.

Former Vice President of Alliance Bank Charged with Bank Fraud

During this reporting period in the U.S. District Court for the District of Minnesota, the former vice president of Private Banking, Alliance Bank, New Ulm, Minnesota, was charged with one count of conspiracy, three counts of forged securities, seven counts of embezzlement by a bank officer, and four counts of mail fraud. The defendant was a primary lending officer at the bank's Edina branch office where she specialized in larger commercial loans and lending to borrowers of higher net worth. Alliance Bank management terminated her employment based on



questionable lending judgment and unauthorized lending that caused losses in excess of \$1.1 million.

In late 2005, an internal bank investigation uncovered numerous defalcations attributed to the defendant and two other senior bank employees. According to the indictment, the defendant used her position as a loan officer to divert for her own use funds that customers paid to the bank as well as fictitious fees she tricked customers into paying. At times, she forged check signatures and endorsements. In an attempt to conceal her embezzlement, the defendant altered bank records and made false statements when questioned by bank employees about specific transactions. Over a 4-year period, the defendant and two co-conspirators used the money obtained through this scheme for vacations, home renovations and decorating, automobiles, cosmetic surgery, gambling, and country club dues. The defendant and her co-conspirators embezzled approximately \$1 million from the bank and its customers.

As previously reported, the other two co-conspirators, the former branch president/chief lending officer and the former vice president of commercial lending, pleaded guilty to theft, embezzlement, or

misapplication by a bank officer for their involvement in the scheme.

Joint investigation by the FDIC OIG and FBI, based on a referral from DSC; prosecution is being handled by the U.S. Attorney's Office for the District of Minnesota.

Bank Employee Indicted for Stealing Over \$3.2 Million from BancFirst

On February 16, 2007, the former vault teller and teller supervisor at a branch office of BancFirst in Seminole, Oklahoma, was indicted in the U.S. District Court for the Eastern District of Oklahoma, on 98 counts of false entries in the books of an FDIC-insured bank, one count of bank fraud, and one count of criminal forfeiture. The criminal forfeiture included a money judgment of \$3,263,695, forfeiture of real property, including 11 motor vehicles and tractors, electronic entertainment equipment, furniture, and jewelry.

The defendant was employed at BancFirst from June 1999 to on or about June 3, 2005. In her capacity, she controlled the flow of money in and out of the branch's vault, teller drawers, and automated teller machines; prepared the daily vault cash reconciliation reports; and was responsible for reconciling several general ledger accounts within



the Seminole branch, including the branch cash account and the branch cash in transit account.

The indictment alleges that the defendant created false internal bank documents, which purported to show the movement of cash in and out of the branch vault, and then, separately created false internal bank documents to cure the account imbalances caused by her initial false entries. The defendant also prepared, and caused to be delivered to BancFirst management, false vault cash reconciliation reports, which overstated the amount of cash in the branch vault. The indictment also alleged the defendant received approximately \$3,263,695 from her criminal activity.

Joint investigation by the FDIC OIG and the FBI; prosecution is being handled by the United States Attorney's Office for the Eastern District of Oklahoma.

Bank Customer Sentenced to 8 Years in Prison for \$18 Million Bank Fraud

On November 1, 2006, in the U.S. District Court for the Northern District of Illinois, a bank customer of Lincoln State Bank was sentenced to 97 months of incarceration, to be followed by 5 years of supervised release and was ordered to pay \$18.8 million in restitution. The

defendant earlier pleaded guilty in July 2006 to a criminal information charging him with one count of bank fraud. The defendant admitted to devising a scheme to divert over \$18 million of loan proceeds from creditors.

According to the information, the defendant defrauded two financial institutions of loan payments owed by third-party borrowers. The defendant submitted falsified loan payment documents and financial reports to Lincoln State Bank, an FDIC-regulated institution, and Ottawa Savings Bank, an Office of Thrift Supervision-regulated institution. Both financial institutions were FDIC insured.

These diverted funds represented proceeds/payments against participation loan agreements between third-party borrowers and 15 financial institutions. Commercial Loan Corporation, Inc., Oak Brook, Illinois, a company controlled by the defendant, brokered commercial loans between the affected borrowers and lenders. As part of this service, Commercial Loan Corporation, Inc., provided collection/payment services for the borrowers. The defendant's scheme involved: collecting and diverting loan payments owed to creditors, and overselling the loan participation agreements to other



financial institutions to obtain funds in excess of the borrowers' approved loans. These loan payments and excess funds were then diverted, for the defendant's personal benefit, into a manufacturing plant as capitalization loans. The defendant's diverted funds were lost when the plant closed and these "loans" went into default.

Joint investigation by the FDIC OIG and the FBI, based on a referral from DSC; prosecuted by the U.S. Attorney's Office for the Northern District of Illinois, Eastern Division.

Universal Federal Savings Bank Customer Sentenced and Ordered to Pay \$9.7 Million in Restitution

On January 16, 2007, in the U.S. District Court for the Northern District of Illinois, a former customer of Universal Federal Savings Bank (Universal) was sentenced to 42 months of incarceration, to be followed by 5 years of supervised release and 300 hours of community service. The defendant was also ordered to pay restitution in the amount of \$9,750,545 to the FDIC and \$707,280 to the five Ponzi scheme victims. In July 2006 the defendant pleaded guilty to one count of wire fraud affecting a financial institution. The guilty plea is the result of an indictment filed in January 2005 concerning the

activities surrounding the failure of Universal on June 27, 2002.

As previously reported, the indictment alleged that the Universal customer conspired with Universal's chief operations officer to misapply the financial institution's funds and to make a false entry in a book, report, or statement of or to Universal. The scheme and conspiracy caused a loss in excess of \$10 million, and Universal was forced to cease operations.

The chief operations officer was earlier sentenced to 38 months' incarceration, to be followed by 3 years' supervised release, and 600 hours of community service. She was also ordered to pay restitution in the amount of \$1,313,082 to the FDIC.

Joint investigation by the FDIC OIG and the FBI based on a referral from DSC; prosecuted by the U.S. Attorney's Office for the Northern District of Illinois.

Real Estate Frauds

The increased reliance by both financial institution and non-financial institution lenders on third-party brokers has created opportunities for fraud. According to the FBI, mortgage fraud is one of the fastest growing white-collar crimes. Such illegal activity can cause financial ruin to



homeowners and local communities. It can further impact local housing markets and the economy at large. Mortgage fraud can take a variety of forms and involve multiple individuals, but most cases involve inflating the value of a property for more than its worth, with scammers pocketing the difference. Several investigations during the reporting period addressed fraudulent mortgage and real estate schemes, as discussed below.

Mortgage Fraud Investigation Leads to Charges Against Multiple Defendants in the Northern District of Georgia


The OIG’s ongoing investigation of mortgage fraud and land flip schemes orchestrated by multiple subjects operating in Georgia, Florida, Texas, South Carolina, North Carolina, and Nevada has resulted in a flurry of guilty pleas. We initiated the investigation based on a referral from DSC’s Atlanta Regional Office. Several FDIC-regulated institutions have been victimized in the mortgage fraud schemes.

To illustrate, on December 14, 2006, the former senior vice president of Mortgage Operations at nBank, an OCC-regulated institution in Commerce, Georgia, was charged and pleaded guilty in the U.S. District Court

for the Northern District of Georgia to a one-count criminal information charging him with defrauding nBank of between \$7.5 and \$11 million. On the same date, a mortgage broker and his company, Infinity Mortgage, Atlanta, Georgia, also pleaded guilty to one count of bank fraud for their role in defrauding nBank of \$1.8 million in a mortgage fraud scheme.

The mortgage broker, acting on behalf of Infinity Mortgage, submitted and received short-term funding for 23 loans totaling approximately \$1.835 million from nBank. These 23 loans were placed on Infinity Mortgage’s Warehouse line of credit at nBank. The loans were to stay on the nBank line for a short period of time while the mortgage broker found qualified investors to purchase the loans.

The mortgage broker was unable to find qualified investors to purchase the 23 loans, and the loans became aged on nBank books. In order to remove the aged loans from the line of credit, the mortgage broker, with the knowledge and at the direction of the former senior vice president, submitted 23 new loan packages that contained false and fraudulent information. The mortgage broker’s “rolling” of the loans allowed nBank to remove the aged loans from its



books; however, the 23 new loans eventually were found to be fraudulent loans and nBank wrote them off. The senior vice president knew of and participated in this “rolling” scheme with the mortgage broker and several other mortgage lenders.

On December 18, another mortgage broker and Southern Lenders Mortgage Corporation (Southern Lenders), a company the mortgage broker formerly co-owned in Newnan, Georgia, pleaded guilty to bank fraud in the Northern District of Georgia for their role in a mortgage fraud scheme. The guilty pleas are the result of an earlier indictment charging the mortgage broker and Southern Lenders with one count of bank fraud for defrauding nBank of approximately \$3.7 million.

The mortgage broker, acting on behalf of Southern Lenders, submitted and received short-term funding for 34 loans totaling approximately \$3.7 million from nBank. These 34 loans were placed on Southern Lenders Warehouse line of credit at nBank. The loans were subsequently sold by Southern Lenders to several investors on the secondary market. In the normal course of business, when such loans are sold, the investors would wire the loan proceeds, and the bank should have received the proceeds

directly from the investors. However, with the knowledge and consent of the former senior vice president of Mortgage Operations at nBank, the end investors, at the direction of the mortgage broker, wire transmitted the loan proceeds to a bank account in the name of the mortgage broker, doing business as J.P. Enterprises.

Joint investigation by the FDIC OIG and the FBI based on a referral from DSC; prosecuted by the U.S. Attorney’s Office for the Northern District of Georgia.

Conviction in Mortgage Fraud Trial in Dallas, Texas

On March 19, 2007, following a trial that began February 21, a federal jury in Dallas convicted a purported real estate investor on all 14 counts in a March 2006 indictment charging him for his role in orchestrating a mortgage fraud scheme. Specific charges included bank fraud, wire fraud, and engaging in monetary transactions derived from specified unlawful activity. A second defendant in the case, a loan broker, earlier pleaded guilty to one count of wire fraud for his role in the scheme. A third defendant, a loan officer, was acquitted of the six counts charged against her in the indictment.

The indictment alleged that the three associates devised a scheme



to fraudulently obtain 21 mortgage loans totaling \$3,220,550. The defendants used schemes commonly referred to in the mortgage industry as property flips, markups and kickbacks, and HUD swaps to facilitate the mortgage fraud. One of the mortgage companies impacted by this fraud scheme was Fremont Investment & Loan, an FDIC-supervised institution in Brea, California.

In each instance, one of the defendants convinced inexperienced real estate investors to stand in as straw borrowers and purchase the properties for fraudulently inflated sales prices. A second defendant, a loan officer, and the third, a mortgage broker, knowingly submitted false documentation to the lenders to enable the straw borrowers to qualify for the mortgage loans. Each of the straw borrowers received a financial inducement for participating in the fraud scheme. Fraudulent real estate appraisals were also submitted to the lenders to support the inflated sales prices of the properties.

Joint investigation by the FDIC OIG and the FBI; prosecuted by the U.S. Attorney's Office for the Northern District of Texas.

Defendants Found Guilty in \$2.16 Million Real Estate Fraud

On December 12, 2006, following a 2-week trial in the U.S. District Court for the Northern District of Texas, a jury found two defendants guilty of all counts in an October 3, 2006, superseding indictment charging them with conspiracy, mail fraud, wire fraud, bank fraud, and aiding and abetting for their roles in a mortgage fraud scheme. Two other defendants earlier pleaded guilty for their participation in the scheme.

Three of the defendants operated various companies in the Dallas area for the purported purpose of remodeling and marketing investment properties. The fourth defendant was an escrow officer for two Dallas area title companies. From December 2002 through March 2004, the four men engaged in a real estate scheme to defraud various real estate lenders, buyers, and sellers, including Fremont Investment & Loan. Three of the defendants located single-family residences and recruited straw purchasers and borrowers to purchase and finance the residences. Fraudulent loan documents were then submitted to the lenders in the name of the straw borrowers falsely indicating the down payment for the loans had been made

by the borrowers. The fourth defendant, as an employee of the title company, would release the loan proceeds early to the three others, who would then purchase cashier's checks in the name of the straw borrowers for the requisite down payment. The defendants caused inflated loan amounts to be funded by mortgage lenders and financial institutions, and conspired to distribute the fraudulently obtained loan proceeds

among themselves and others. Three of the defendants also executed contracts between their company, Better Homes of Dallas, and the straw borrowers, stating the company would be responsible for the loans, but they later failed to fulfill their contract.

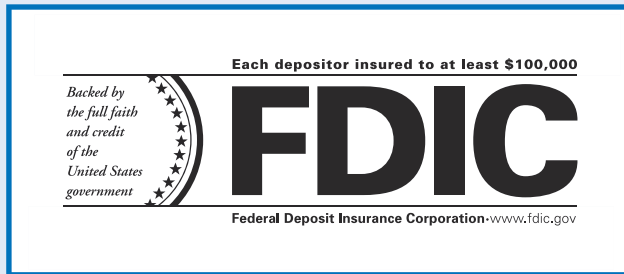
Joint investigation by the FDIC OIG and the FBI; prosecuted by the U.S. Attorney's Office for the Northern District of Texas.

A Strong Partnership

The OIG has partnered with various U.S. Attorneys' Offices throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the U.S. Attorneys' Offices have yielded positive results during this reporting period.

Our strong partnership has evolved from years of trust and hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the nation's financial system.

For the current reporting period, we are especially appreciative of the efforts of the Assistant U.S. Attorneys in the following offices: Southern District of Florida, Western District of Tennessee, Northern District of Illinois, District of Colorado, District of Nebraska, Eastern District of Kentucky, Eastern District of Missouri, District of Minnesota, Middle District of Georgia, Northern District of Illinois—Eastern Division, Northern District of Iowa, Eastern District of Texas, District of Massachusetts, Southern District of Texas, Northern District of Iowa, and the Southern District of Illinois.



Strategic Goal 2

Insurance: Help the FDIC Maintain the Viability of the Insurance Fund

Federal deposit insurance remains a fundamental part of the FDIC's commitment to maintain stability and public confidence in the nation's financial system. In February 2006, President Bush signed into law the Federal Deposit Insurance Reform Act of 2005, prompting sweeping changes in the federal deposit insurance system. The Congress gave the Corporation 9 months to implement most of the provisions of the legislation. In October 2006, the FDIC Board of Directors approved a final rule to implement a one-time assessment credit to banks and thrifts. The credit will be used to offset future assessments charged by the FDIC and will recognize contributions that certain institutions made to capitalize the funds during the first half of the 1990s. In November 2006, the Board also adopted a final rule on the pricing structure and approved a more risk-sensitive framework for the 95 percent of insured institutions that are well capitalized and well managed.

In addition to the extensive rulemaking required in conjunction with deposit insurance reform, fundamental changes were made in the FDIC's business functions, including modification to major application systems and creation of

new on-line tools. System changes in support of deposit insurance reform will continue in 2007.

The continuing consolidation of the banking industry means there are a few very large institutions that represent an increasingly significant share of the Deposit Insurance Fund's risk exposure. Industry consolidation presents benefits and risks to the Deposit Insurance Fund. While the risks to the funds are diminished because of the diversification benefits of consolidation (along geographic and product lines), the concentration of deposits in fewer insured depository institutions increases the risks to the Deposit Insurance Fund in the event a large insured depository institution fails.

As a result of industry consolidation, the assets in the industry are also increasingly concentrated in a small number of large, complex institutions for which the FDIC is not, for the most part, the primary supervisor. The largest banks operate highly complex branch networks, have extensive international and capital market operations, and work on the cutting edge of technologically sophisticated finance and business. The increased complexity of the industry and the concentration of risk to the insurance funds in the largest

banking organizations are expected to grow more pronounced over time and to present greater risk-management challenges to the Corporation. A two-tiered banking system characterized by a limited number of very large, complex institutions and a much larger number of small community banks appears to be emerging. The banking regulators, including the FDIC, need insight into the risks that are inherent in these different types of banking organizations.

To help the FDIC maintain the viability of the deposit insurance fund, the OIG's 2007 performance goal is as follows:

- Evaluate corporate programs to identify and manage risks in the banking industry that can cause losses to the fund.

OIG Work in Support of Goal 2

As insurer, the FDIC needs a comprehensive understanding of the risks that the largest institutions pose to the Deposit Insurance Fund. The FDIC is not the primary federal regulator for most of the large institutions that it insures. Therefore, the risk assessment process is based on a combination of information obtained from the primary federal regulator, the institution, supervisory activities, market data, and publicly available data. The FDIC established the Large Bank Branch in headquarters to coordinate the FDIC's nationwide programs focused on supervising and assessing risk in large institutions. A key program in this regard is the Dedicated Examiner Program, established in 2002. This program has placed dedicated examiners in the six largest insured depository institutions to work in

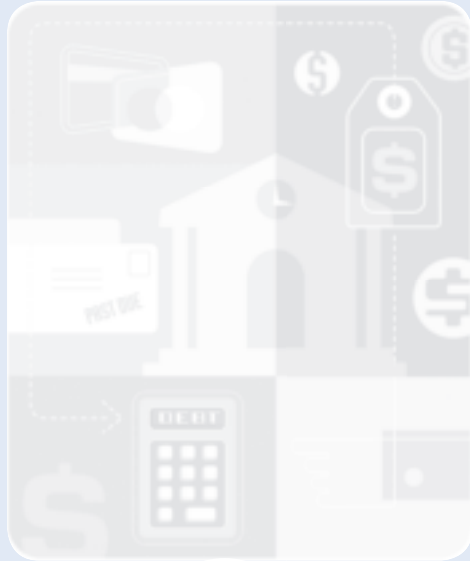
cooperation with primary supervisors and bank personnel to obtain real-time access to information about the risk and trends in those institutions. We are currently conducting an audit to determine whether the Dedicated Examiner Program is contributing to the FDIC's efforts to assess and quantify the risks posed by large institutions to the Deposit Insurance Fund.



Another of our audits is assessing the FDIC's role in reviewing shared national credits (SNC) and the consideration of SNC ratings in risk management examinations of FDIC-supervised institutions. SNCs represent the largest and most complex loans and loan commitments held by FDIC-insured institutions.

OIG Work Cited in GAO Studies

The Federal Deposit Insurance Reform Conforming Amendments Act of 2005, which the President signed into law on February 15, 2006, contains necessary technical and conforming changes to implement deposit insurance reform, as well as a number of study and survey requirements. In fulfillment of some of those requirements, the U.S. Government Accountability Office issued three reports in February 2007. The FDIC OIG's work is referenced in two of the three GAO studies. One of GAO's reports is entitled, *FDIC: Human Capital and Risk Assessment Programs Appear Sound, but Evaluations of Their Effectiveness Should Be Improved*. In this report, GAO referenced findings in our earlier report on FDIC reserve ratio and assessment determinations and also cited prior OIG work related to possible insurance fund losses if a so-called "megabank" were to fail. In the second GAO report entitled, *Deposit Insurance: Assessment of Regulators' Use of Prompt Corrective Action Provisions and FDIC's New Deposit Insurance System*, GAO made several references to issues presented in two of our earlier reports on the role of prompt corrective action as part of the enforcement process and the effectiveness of prompt corrective action provisions in preventing losses to the deposit insurance funds.



Strategic Goal 3:

Consumer Protection: Assist the FDIC to Protect Consumer Rights and Ensure Customer Data Security and Privacy

Consumer protection laws are an important part of the safety net of America. The U.S. Congress has long advocated particular protections for consumers in relationships with banks. For example:

- The Community Reinvestment Act encourages federally insured banks to meet the credit needs of their entire community.
- The Equal Credit Opportunity Act prohibits creditor practices that discriminate based on race, color, religion, national origin, sex, marital status, or age.
- The Home Mortgage Disclosure Act was enacted to provide information to the public and federal regulators regarding how depository institutions are fulfilling their obligations towards community housing needs.
- The Fair Housing Act prohibits discrimination based on race, color, religion, national origin, sex, familial status, and handicap in residential real-estate-related transactions.
- The Gramm-Leach-Bliley Act eliminated barriers preventing the affiliations of banks with securities firms and insurance companies and mandates new privacy rules.

- The Truth in Lending Act requires meaningful disclosure of credit and leasing terms.
- The Fair and Accurate Credit Transactions Act further strengthened the country's national credit reporting system and assists financial institutions and consumers in the fight against identity theft.

The FDIC carries out its role by (1) providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations and (2) examining the banks where the FDIC is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment.

FDIC Chairman Bair has stressed the importance of economic inclusion and has expressed concern that market mechanisms are not working as well as they should for low-to-moderate income families who must often pay high amounts for basic financial services that others obtain at far less cost. Many people lack the financial skills needed to analyze and compare products and their prices. Oftentimes the problem is the lack of disclosures that describe a product and its true



costs in fair and simple terms. Another factor could be linked to aspects of safety and soundness regulation that could unnecessarily deter banks from serving the needs of their communities or create conditions that favor high-cost products. To address these concerns, in addition to the FDIC's existing Money Smart program, the Corporation has undertaken two initiatives—a military lending initiative and a newly created Advisory Committee on Economic Inclusion. As the Chairman has pointed out, continuing dialogue among consumer advocates, regulators, and the banking industry is key to the challenge of closing the gap between what the unbanked and underbanked pay for credit and what those in the mainstream pay. In recent testimony before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, the Chairman focused on strengthening protections available to borrowers in the subprime mortgage market and ensuring that predatory lending practices do not take root in the banking system.

The OIG's role under this strategic goal is targeting audits and evaluations that review the effectiveness of various FDIC programs aimed at protecting consumers, fair lending, and

community investment. Additionally, the OIG's investigative authorities are used to identify, target, disrupt, and dismantle criminal organizations and individual operations engaged in fraud schemes that target our financial institutions.

To assist the FDIC to protect consumer rights and ensure customer data security and privacy, the OIG's 2007 performance goals are as follows:

- Evaluate the effectiveness of FDIC programs for ensuring customer data security and privacy at FDIC-insured institutions.
- Review the FDIC's examination coverage of institution compliance at FDIC-insured institutions.
- Address allegations of fraudulent insurance coverage and identity theft schemes affecting the FDIC.

OIG Work in Support of Goal 3

Several audits completed during the reporting period addressed important consumer protection matters: security of sensitive customer information and community reinvestment reporting. Investigative work related to protection of personal information and misrepresentation of deposit insurance complemented audit efforts in this strategic goal area, as described below.



IT Examination Coverage of Financial Institutions' Oversight of Technology Service Providers

In the first 10 months of 2006, over half of the 213 information security breaches reported by financial institutions to the FDIC involved technology service providers (TSP). In accordance with federal laws and regulations, financial institutions must safeguard sensitive customer information against unauthorized disclosure when outsourcing various IT operations to TSPs.

Interagency guidelines contained in the FDIC Rules and Regulations establish key controls over TSPs, noting that each bank shall (1) exercise due diligence in selecting TSPs, (2) have contractual arrangements with their TSPs that require appropriate measures to safeguard customer information, and (3) provide ongoing monitoring of TSPs to ensure they have satisfied their contractual obligations.

We conducted an audit to assess DSC's (1) IT examination procedures for addressing the security of sensitive customer information when FDIC-supervised institutions use TSPs and (2) examiners' implementation of those procedures.

We determined that the FDIC can

achieve greater assurance that financial institutions are ensuring that TSPs safeguard customer information. We recommended that the FDIC: (1) revise IT-RMP guidance to ensure that examiners adequately assess financial institution compliance with the interagency guidelines pertaining to the oversight of TSPs and (2) reemphasize the need for examiners to clearly document decisions and supporting logic for the approach used in assessing compliance with the interagency guidelines related to TSPs as well as support for examiner conclusions. These measures will help in protecting customers from identity theft and institutions from fraud and reputational and other risks associated with unauthorized access to or use of customer information.

FDIC management agreed with both recommendations, noting that it would incorporate our recommendations into its planned evaluation of first year performance under the IT-RMP.

FDIC's Implementation of the 2005 Amendments to the Community Reinvestment Act Regulations

The purpose of the Community Reinvestment Act of 1977 (CRA) was to encourage depository institutions



to help meet the credit needs of the communities in which they operate, including low- and moderate-income neighborhoods, consistent with safe and sound banking practices. The CRA has come to play an important role in improving access to credit among under-served rural and urban communities.

The CRA requires that each insured depository institution's record in helping meet the credit needs of its entire community be periodically evaluated and publicly reported. In 2005, the federal banking agencies amended their CRA regulations which created a new class of small institutions (intermediate small banks, or ISBs) with reduced CRA reporting requirements and more flexibility in meeting CRA goals.

During the reporting period, we conducted an audit to determine whether the FDIC has (1) issued institution and examination guidance that addresses the 2005 amendments to the CRA regulations and (2) established outcome-oriented performance measures to determine if the amended regulations have provided the intended regulatory relief for smaller community banks and preserved the importance of community development.

We found that the FDIC has issued institution and examination guidance that addresses the 2005 amendments to the CRA regulations. The institution guidance was supplemented with interagency questions and answers guidance in March 2006. Additionally, our review of 10 ISB Performance Evaluation (PE) reports found that examiners had generally followed the new examination procedures, using the lending and community development tests to assess ISBs. However, we noted one area where examiner guidance could be improved regarding the implementation of the ISB community development test and the presentation of the results in the PE reports to support test conclusions.

Also, it may be premature to establish outcome-oriented performance measures for the amendments made to the CRA regulations. Still, developing a strategy to determine whether the 2005 amendments to the CRA regulations have provided the intended regulatory relief for smaller community banks and preserved the importance of community development will allow the FDIC to proactively assess the impact of the amendments made to the CRA regulations.

We therefore recommended that the Director, DSC, (1) enhance examiner



guidance to ensure examiners provide complete support in the PE reports for their conclusions for the community development test, (2) develop examiner guidelines that incorporate the use of comparative measures within the performance analysis, and (3) develop a strategy for measuring CRA activities as a result of the amendments made to the regulations. DSC management agreed to implement the first recommendation and will raise the remaining two with the other federal banking agencies for interagency consideration.

Ongoing Audit Work

The FDIC uses its compliance examination process to ascertain the effectiveness of an institution's program for complying with consumer protection laws and regulations. DSC compliance examinations combine a risk-based examination process with an in-depth evaluation of an institution's compliance management system, resulting in a top-down, risk-focused examination approach. A financial institution must develop and maintain a sound compliance management system that is integrated into the overall risk management strategy of the institution. Audit work currently underway will determine whether DSC is adequately assessing institutions'

compliance management systems during compliance examinations.

ECU Works to Curtail Identity Theft and Misrepresentation of FDIC Insurance or Affiliation

Identity theft continues to become more sophisticated, and the number of victims is growing. Identity theft includes using the Internet for crimes such as "phishing" emails and "pharming" Web sites that attempt to trick people into divulging their private financial information. Schemers pretend to be legitimate businesses or government entities with a need for the information that is requested. The OIG's Electronic Crimes Unit (ECU) responds to such phishing and pharming scams involving the FDIC and the OIG.

Unscrupulous individuals also sometimes attempt to misuse the FDIC's name, logo, abbreviation, or other indicators to suggest that deposits or other products are fully insured. Such misrepresentations induce the targets of schemes to trust in the strength of FDIC insurance while misleading them as to the true nature of the insurance investments being offered. Abuses of this nature harm consumers and can also erode public confidence in federal deposit



insurance. Our ECU has a role to play in combating such schemes.

During the reporting period, the ECU opened four new cases related to phishing involving the FDIC. In three of the new cases, the ECU was able to have the fraudulent Web sites deactivated. The ECU continues to investigate the fourth new phishing case. The ECU was also able to have three other fraudulent FDIC-related phishing Web sites deactivated that were part of previously opened cases.

Additionally, the ECU investigated two new instances of Web sites that falsely advertised FDIC insurance. In both cases, the ECU was able to have the Web site deactivated or the reference to FDIC insurance removed.

Finally, the ECU continued to work an investigation involving a scam where banks are requested to send confidential information by fax to an entity purported to be the FDIC. The faxes go to a service that converts them to email and sends the information to free, untraceable email addresses. During the reporting period, the ECU had two fax numbers deactivated. The ECU has previously had ten fax numbers associated with this scam deactivated.

OIG Hosts Colombian Delegation

The OIG's work in combating cyber-crime is often of interest to others in the law enforcement community. During the reporting period we hosted a delegation of law enforcement officials from the Colombian National Police. The visit was sponsored by the U.S. State Department's Bureau of Diplomatic Security, Office of Anti-Terrorism Assistance, Cyber-Terrorism Training Program. As part of the State Department's program, the Colombian group visited a number of federal law enforcement entities to gain an understanding of what is required to establish and operate a large-scale investigative function to fight cyber-crimes. Of particular interest to the Colombian group was how the OIG's electronic labs are set up, how the OIG manages evidence in storage, and how the lab deals with a large-scale chain of evidence. The delegation was grateful for the opportunity to visit the FDIC and presented the OIG representatives with U.S. State Department certificates of appreciation for having "made a significant contribution to the government of Colombia's fight against cyber-terrorism."



Strategic Goal 4:

Receivership Management: Help Ensure that the FDIC is Ready to Resolve Failed Banks and Effectively Manages Receiverships

The United States provides protection to depositors in its banks, savings and loan associations, and credit unions. One of the key players in this process is the FDIC. Among its various functions, the FDIC acts as the receiver or liquidating agent for failed FDIC-insured institutions. The success of the FDIC's efforts in resolving troubled institutions has a direct impact on the banking industry and on the taxpayers.

The Division of Resolutions and Receiverships (DRR) exists to plan and efficiently handle the resolutions of failing FDIC-insured institutions and to provide prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.


- The **resolution process** involves valuing a failing federally insured depository institution, marketing it, soliciting and accepting bids for the sale of the institution, determining which bid to accept, and working with the acquiring institution through the closing process.
- The **receivership process** involves performing the closing function at the failed bank; liquidating any remaining assets; and distributing any proceeds to the FDIC, the bank

customers, general creditors, and those with approved claims.

The FDIC's resolution and receivership activities pose tremendous challenges. Today record profitability and capital in the banking industry have led to a substantial decrease in the number of financial institution failures compared to prior years. However, as indicated by the trends in mergers and acquisitions, banks are becoming more complex, and the industry is consolidating into larger organizations. As a result, the FDIC could potentially have to handle a failing institution with a significantly larger number of insured deposits than it has had to deal with in the past.

The change between how the FDIC handled resolutions and receiverships 20 years ago and how it will be handling them 20 years from now will be largely based on learning to anticipate and plan, instead of reacting. Through the development of new resolution strategies within the various DRR business lines, the FDIC must set far-reaching plans for the future to keep pace with a changing industry.

The OIG's role under this strategic goal is targeting audits and evaluations that assess the effectiveness of the



FDIC's various programs designed to ensure that the FDIC is ready to and does respond promptly, efficiently, and effectively to financial institution closings. Additionally, the OIG investigative authorities are used to pursue instances where fraud is committed to avoid paying the FDIC civil settlements, court-ordered restitution, and other payments as the institution receiver. The OIG will also continue to work with FDIC officials to keep abreast of the ongoing efforts being taken by DRR and the Corporation as a whole, to sustain proficiency in resolution activity and to prepare for the possibility of a large institution failure or multiple failures caused by a single catastrophic event.

To help ensure the FDIC is ready to resolve failed banks and effectively manages receiverships, the OIG's 2007 performance goals are as follows:

- Evaluate the FDIC's plans and systems for managing bank resolutions.
- Respond to potential crimes affecting the FDIC's efforts to recover financial losses.

OIG Work in Support of Goal 4

DRR has the primary responsibility for resolving failed FDIC-insured institutions promptly, efficiently, and responsively to maintain public confidence in the nation's financial system. In performing their duties, DRR personnel have access to a wide variety of records containing sensitive information concerning bank employees and customers. Prior OIG work focused on DRR efforts to protect such information in hardcopy form. Currently we are conducting an audit to evaluate the design and implementation of selected controls established by DRR to safeguard sensitive information collected and maintained in electronic form as a result of resolution and receivership activity at FDIC-insured institutions.

With respect to other ongoing work, one of the greatest risks to the Deposit Insurance Fund and public confidence in the nation's financial system would be the failure of a large bank. The FDIC has put plans in place to deal with the possibility of a large bank failure, and in that regard it undertook a Strategic Readiness Project in January 2007. The purpose of the project is to create a simulation that will stress the decision-making associated with a large bank failure, enhance



the FDIC's ability to determine an effective resolution strategy, advance knowledge of the process, and identify lessons learned. A steering committee of FDIC executives is leading the project and Corporate University is directing it. A contractor has been hired to design the simulation. During the reporting period, the OIG has been monitoring the project. We need to be ready for any large failure when fraud is a contributing factor. We also need to be prepared to review the circumstances that cause a large bank failure and make recommendations, if appropriate, to strengthen the regulatory process.

From an investigative standpoint, the sentencing in one of our cases during the reporting period illustrates the nature of the work we do in concealment of assets investigations to protect the FDIC's interests as receiver of a failed institution, as discussed below. We do such work in furtherance of our performance goal related to the FDIC's efforts to recover financial losses.

Former CEO of Sunbelt Savings Sentenced to 8 Years in Prison

On October 20, 2006, in the U.S. District Court for the Northern District of Texas, the former Chief Executive Officer (CEO) of the now defunct Sunbelt Savings and Loan of Dallas, Texas, was sentenced to 97 months' incarceration and ordered to pay a criminal forfeiture of \$2,054,366 to the U.S. Government and restitution in the amount of \$312,828 to the FDIC.

After a week-long trial in January 2006, the former CEO was convicted on all 27 counts of a superseding indictment that charged him with 6 counts of mail fraud, 11 counts of making false statements, 9 counts of concealing assets from the FDIC, and one count of money laundering. At a separate hearing, the court found that the former CEO was subject to \$2,054,366 in cash forfeitures.

The former CEO pleaded guilty in 1990 to federal fraud charges in connection with the collapse of Sunbelt, which lost approximately \$2 billion during the 1980s. In the criminal case against him, he was ordered to pay back \$7.5 million to the FDIC and \$8.5 million in a civil judgment. His plea agreement required him to relinquish a



portion of his income to repay the obligation, with the percentage increasing as income increased.

Going back to July 1993, the former CEO engaged in a scheme to defraud the FDIC of its payments by creating a trust, known as the Oslin Nation Trust. The former CEO used the trust to conceal earnings from his business, and pay his personal and legal expenses, and accounting fees. The former CEO made false monthly reports to the U.S. Probation Office to conceal hundreds of thousands of dollars from the FDIC in order to avoid the payments required by the FDIC restitution order.

We investigated this case with assistance from the FDIC Legal Division. The U.S. Attorney's Office for the Northern District of Texas prosecuted the case.



Strategic Goal 5: **FDIC Resources** **Management: Promote** **Sound Governance and** **Effective Stewardship** **and Security of Human,** **Financial, IT, and** **Physical Resources**

The FDIC manages and utilizes a number of critical strategic resources to carry out its mission successfully, particularly its human, financial, IT, and physical resources. The Corporation does not receive an annual appropriation, except for its OIG, but rather is funded by the premiums that banks and thrift institutions pay for deposit insurance coverage, the sale of assets recovered from failed banks and thrifts, and from earnings on investments in U.S. Treasury securities.

The Board approved a \$1.1 billion corporate operating budget for 2007, approximately 4.6 percent higher than for 2006. The approved budget provides funding for additional compliance examiners, increased employee training, enhanced IT security and privacy programs, and completion of systems changes required to support the implementation of deposit insurance reform. The Corporation's 2007 spending on multi-year investment projects separately approved by the Board is expected to be approximately \$19 million to \$23 million.

The Corporation is continuing to operate in the context of its New Financial Environment, intended to meet current and future financial management and financial information needs; improve corporate financial

business processes; and redirect resources from transaction processing to analysis, risk management, and decision support.

Financial resources are but one aspect of the FDIC's critical assets. The Corporation's human capital is also vital to its success. Because of the projected retirements of a large number of long-serving employees, the FDIC has made efforts to reshape its workforce with the implementation of the Corporate Employee Program, the Succession Management Program, and the Leadership Development Program. Throughout the reshaping of its workforce, the FDIC maintains its commitment to a working environment of high integrity and to the achievement of its mission.

Technological advances have produced tools that all workers today would be lost without. IT drives and supports the manner in which the public and private sector conduct their work. At the FDIC, the Corporation seeks to leverage IT to support its business goals in insurance, supervision and consumer protection, and receivership management, and to improve the operational efficiency of its business processes. The financial services industry employs technology for similar purposes.



Along with the positive benefits that IT offers comes a certain degree of risk. In that regard, information security has been a long-standing and widely acknowledged concern among federal agencies. The E-Government Act of 2002 recognized the importance of information security. Title III of the E-Government Act, entitled the Federal Information Security Management Act, requires each agency to develop, document, and implement an agency-wide information security program to provide adequate security for the information and information systems that support the operations and assets of the agency. Section 522 of the Consolidated Appropriations Act of 2005 requires agencies to establish and implement comprehensive privacy and data protection procedures and have an independent third-party review performed of their privacy programs and practices.

Business continuity and disaster recovery are foremost concerns to all federal agencies. The FDIC must be sure that its emergency response plans provide for the safety and physical security of its human resources and ensure that its business continuity planning and disaster recovery capabilities keep critical business functions

operational during any emergencies, including threats to public health such as a pandemic influenza.

The Federal Deposit Insurance Act empowers the FDIC to enter into contracts to procure goods and services. Over the past several years, the Corporation has increased its reliance on outsourcing for services such as IT infrastructure support, IT application system development, and facilities maintenance. As of March 2006, the value of the FDIC's active contracts totaled over \$1.6 billion. Also, a number of new contracting vehicles have been implemented. For example, the Corporation combined approximately 40 IT-related contracts into one contract with multiple vendors for a total program value of approximately \$555 million over 10 years. Also for the first time the FDIC used a large technical infrastructure contract through the General Services Administration valued at over \$340 million over 5 years.

As an integral part of its stewardship of the insurance funds, the FDIC has established a risk management and internal control program. The Office of Enterprise Risk Management (OERM) is the corporate oversight manager for internal controls and risk management.



OERM works in partnership with all FDIC divisions and offices, helping them to identify, evaluate, monitor, and manage their risks.

To promote sound governance and effective stewardship of FDIC strategic resources, the OIG's 2007 performance goals are as follows:

- Evaluate corporate efforts to fund operations efficiently, effectively, and economically.
- Assess corporate human capital strategic initiatives.
- Promote integrity in FDIC internal operations.
- Promote alignment of IT with the FDIC's business goals and objectives.
- Promote IT security measures that ensure the confidentiality, integrity, and availability of corporate information.
- Promote personnel and physical security.
- Evaluate corporate contracting efforts.
- Monitor corporate risk management and internal control efforts.

OIG Work in Support of Goal 5

The FDIC's Succession Planning Efforts

Our Evaluations group conducted a review of the FDIC's succession planning efforts to identify and address future critical staffing and leadership needs. We evaluated whether the FDIC's succession planning initiatives were consistent with the seven key principles for effective succession planning management identified by GAO, the Office of Personnel Management, the Corporate Leadership Council, and the National Academy of Public Administration.

We found that the FDIC has recently put initiatives in place and is developing others that are consistent with seven key principles:

- Commitment and active support of top leadership.
- A direct link between the organization's mission and its strategic plan and outcomes.
- Identification of the critical skills and competencies that will be needed to achieve current and future programmatic goals.
- Development of strategies to address gaps in mission critical and other key positions.



- Leadership training programs that include formal and informal training for all levels of supervisors, managers, and potential leaders.
- Strategies for addressing specific human capital challenges, such as diversity, leadership capacity, and retention.
- A process for evaluating the costs and benefits of succession planning efforts and the return on investment it provides for the organization.

We limited the results of this review to describing and providing the status of the FDIC's current and planned initiatives. We did not make recommendations but noted in the report that the initiatives should be assessed at a later date to determine their effectiveness in achieving the desired outcomes.

FDIC's Contract Planning and Management for Business Continuity

The Federal Emergency Management Agency has issued guidance for agencies to use in developing continuity of operations plans. The FDIC's Emergency Preparedness Program establishes the FDIC's business continuity policy and requires Business Continuity Plans (BCP) to be established in the FDIC's headquarters

and regional offices. The BCPs include procedures for relocating essential personnel; resuming and restoring FDIC critical business processes; and recovering and reconstituting supporting IT systems. Identifying essential contracts and ensuring that contracts provide for services in the event of a BCP scenario are critical to FDIC operations.

We conducted an audit to determine whether the FDIC has planned for essential contract services to be provided in the event of an emergency that requires implementation of the FDIC's BCP. We reported that the FDIC has done so and is continuing to improve contract management for business continuity. It has identified most essential contracts for business continuity purposes and modified many of those contracts to include emergency preparedness clauses. It also has a process in place to update its list of essential contracts in the BCP annually.

We noted that the FDIC could further improve its contract planning and management for business continuity by:

- enhancing BCP procedures and the Business Impact Analysis questionnaire to require documentation of all essential contracts, including detailed information about each contract;



- requiring program offices to include emergency preparedness clauses in the Statement of Work for essential contracts and subcontracts to ensure that business continuity is considered in the procurement process; and
- amending acquisition policy and procedures and BCP policy to require that essential contractors (a) have emergency plans for providing services to the FDIC in the event of a disruption of normal operations and (b) participate in the FDIC's business continuity testing, training, and exercise activities.

We made three recommendations. Management concurred and quickly completed corrective actions to address our concerns.


FDIC's Compliance with Section 522 of the Consolidated Appropriations Act, 2005

We contracted with KPMG LLP (KPMG) to audit the FDIC's compliance with section 522 of the Consolidated Appropriations Act, 2005. Section 522 requires, among other things, that agencies establish and implement comprehensive privacy and data protection procedures and have an independent third-party

review performed of their privacy programs and practices. The objective of the section 522 audit was to (1) evaluate the FDIC's use of information in an identifiable form (IIF) and the FDIC's privacy and data protection procedures and (2) recommend strategies and specific steps to improve the FDIC's privacy and data protection management practices.

In fulfilling its legislative mandate of insuring deposits, supervising financial institutions, and managing receiverships, the FDIC creates and acquires a significant amount of IIF. Such IIF includes names, addresses, Social Security numbers, phone numbers, dates of birth, and credit report information. Much of the information managed by the FDIC falls within the scope of several statutes and regulations intended to protect such information from unauthorized disclosure.

We reported that the FDIC has established a corporate-wide privacy program to protect the IIF it manages from unauthorized disclosure and ensure its appropriate use consistent with section 522. Of particular note, the FDIC has appointed a Chief Privacy Officer with overall responsibility for the FDIC's privacy program, issued or drafted policies



and procedures for safeguarding IIF, and posted a privacy statement on the FDIC's public Web site. Additionally, the FDIC has performed privacy impact assessments on its systems identified as containing IIF, completed required Privacy Act-related reviews, and implemented mandatory Web-based privacy awareness training for its employees and contractors. Further, the FDIC was working to complete a number of key initiatives to strengthen its privacy program policies, procedures, and practices and ensure compliance with federal privacy-related statutes, policies, and guidelines.

Consistent with the intent of section 522, our report identifies areas of the FDIC's privacy program warranting continued management attention and recommends strategies and specific steps that management should take to ensure adequate protection of its IIF.

Our report recommended that the Chief Privacy Officer:

- enhance the FDIC's privacy program by integrating key ongoing and planned program control activities into a formal documented plan;
- implement additional measures to ensure that IIF is properly secured;
- place additional emphasis on

employee and contractor awareness to physically safeguard IIF in their custody;

- ensure that privacy impact assessments posted on the FDIC's public Web site adequately describe the FDIC's collection and use of IIF; and
- enhance the FDIC's systems development life cycle processes to fully address privacy.

The FDIC agreed with the recommendations and is taking responsive actions.

Interagency Agreement with the General Services Administration for the Infrastructure Services Contract

In March 2004, the FDIC entered into an interagency agreement with the General Services Administration (GSA) for IT support services. Under GSA's Federal Systems Integration Management Center (FEDSIM) Millennia contract, GSA issued the Infrastructure Services Contract (ISC) to SRA International, Inc. (SRA) for IT support services for the Corporation. According to the Board Case approved by the FDIC's Board of Directors, the contract consolidated 37 FDIC infrastructure support contracts. The ISC's approved total value, including



four 1-year contract option periods, is \$357 million. The FDIC's Division of Information Technology (DIT) has assumed responsibility for contract management and oversight.

We conducted an audit to determine whether (1) controls are adequate to ensure that work performed under the ISC complies with the contract's terms and conditions and (2) this contracting method has produced the intended results. We determined that the combination of controls established by the FDIC and those assigned to FEDSIM through the interagency agreement were adequate to ensure that work under the ISC complied with the contract terms and conditions. Also, the ISC has substantially achieved the Corporation's desired results, as presented in the Board Case.

The report makes three recommendations intended to strengthen DIT's monitoring and oversight. DIT management concurred with the recommendations and will document the activities to provide a more structured methodology for evaluating the ISC's performance; establish a process for presenting and obtaining senior management approval for contract line item allocations; and develop a process for conducting periodic program-wide reviews to

assess the reasonableness of the ISC staffing and management plans. Management's planned actions are responsive to our recommendations.

Management Report: Independent Evaluation of the FDIC's Information Security Program-2006

We issued a report to management with more detailed information regarding certain security control concerns identified in our September 2006 report entitled, *Independent Evaluation of the FDIC's Information Security Program-2006*. We made recommendations for control improvements, where appropriate. The report contains sensitive information regarding information security and is not publicly available.

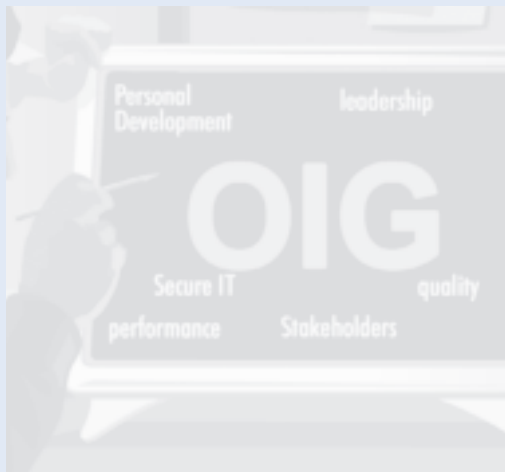
OIG Policy Reviews

During the reporting period, we reviewed 21 draft corporate policies and raised policy issues for consideration in the following draft documents: Protecting Sensitive Information, Planning and Budget Processes, Emergency Preparedness Program, Student Educational Employment Program, and Express Mail Service. Our comments are incorporated in final policy, as determined by FDIC management.



Ongoing Audit and Evaluation Work

Ongoing work in this strategic goal area includes a review of the Corporation's process for issuing task orders under the \$554.8 million IT application services basic ordering agreements. We are determining whether there is a proper balance between the timely issuance of task orders and the maintenance of proper controls. We are also completing our evaluation of the FDIC's Use of Performance Measures. This review is examining how the FDIC meets requirements of the Government Performance and Results Act and also addresses other performance metrics used by the Corporation. Finally, we are assessing the extent to which the FDIC has implemented an enterprise risk management program consistent with applicable government-wide guidance and implementation of the Office of Enterprise Risk Management's September 2006 circular outlining the FDIC's risk management program.



Strategic Goal 6: OIG Internal Processes: Build and Sustain a High- Quality OIG Work Environment

W

While the OIG is focused on the FDIC's programs and operations, we have an inherent obligation to hold ourselves to the highest standards of performance and conduct. Like any organization, we have processes and procedures for conducting our work; communicating with our clients, staff, and stakeholders; managing our financial resources; aligning our human capital to our mission; strategically planning and measuring the outcomes of our work; maximizing the cost-effective use of technology; and ensuring our work products are timely, value-added, accurate, and complete and meet applicable professional standards.

To build and sustain a high-quality OIG work environment, the OIG's 2007 performance goals are as follows:


- Encourage individual growth through personal development;
- Strengthen human capital management and leadership development;
- Foster good client, stakeholder, and staff relationships;
- Ensure quality and efficiency of OIG audits, evaluations, investigations, and other operations;
- Enhance strategic and annual performance planning and performance measurement; and
- Invest in cost-effective and secure IT.

Encourage Individual Growth Through Personal Development

❖ Completed pilot training and development plans for 2007 for auditors, evaluators, and investigators. The plans reflect a minimum requirement of 44 hours of training to be taken by auditors and program analysts in the Office of Audits (OA) and the Office of Evaluations (OE) and a minimum requirement of 64 hours of training for criminal investigators in the Office of Investigations (OI). Information has been gathered from other OIGs and GAO on existing

training and development programs in the interest of creating long-term training and development plans for OA, OE, and OI.

❖ As part of the communication of the training and development plans, staff are encouraged to attain relevant professional certifications. We held a meeting in March 2006 to discuss the pilot training and development plans and career development plans with OIG executives and managers to underscore our commitment to employee development.



❖ Surveyed the six OIG pilot mentoring program participants regarding their 2006 experience and compiled the feedback. We passed along recommendations to the Inspector General for the future of the OIG mentoring program. In January 2007 we announced the OIG's 2007 mentoring program. The OIG now has 7 mentoring pairs. All 14 mentors and mentorees attended the Corporation's Orientation Program in March 2007 and continue to explore ways to enhance the OIG's mentoring program.

Strengthen Human Capital Management and Leadership Development

❖ The 2007 pilot training and development plans for OIG staff include 8 hours of leadership training for each person. Information is being gathered from Corporate University (CU), other OIGs, and GAO on existing training and development programs, including leadership development programs. We plan to discuss establishing an OIG Leadership Development Program, using the CU Leadership Development Program as a framework for incorporating unique OIG requirements.

❖ Developed an end-of-assignment feedback form for OA and OE that was endorsed by senior OA/OE management and the Inspector General. We communicated the intent of the feedback mechanism, use of the form, retention schedule, and review process. Explained the tool at the March executive and manager meeting. Periodic meetings with staff will be held to assess the success of the process and address any necessary modifications.

❖ Took a number of steps to update the OIG's business continuity and emergency preparedness plans, including updating emergency contact information, designating shelter-in-place rooms in OIG office space in coordination with the Division of Administration, and coordinating with DIT on the installation of telephones in shelter-in-place rooms.

❖ Worked with the OIG Information Security Manager to ensure that all OIG employees have a "Safeword" token. The tokens will allow employees to remotely access the FDIC network in an emergency situation.

❖ Assessed Emergency Response Plans and Business Continuity Plans in place at OIG regions and suggested enhancements.



Foster Good Client, Stakeholder, and Staff Relationships

- ❖ Maintained Congressional working relationships by providing Semiannual Report to the Congress for the 6-month period ending September 30, 2006, communicating with interested congressional parties regarding the OIG's work on Office of Foreign Assets Control and challenges regarding predatory lending, and attending FDIC-related hearings on issues of concern to various oversight committees.

- ❖ Developed OIG congressional protocols and shared draft protocols with the FDIC's Director of the Office of Legislative Affairs, then shared the draft protocols with the FDIC Chairman.

- ❖ Communicated with the Chairman and Vice Chairman through the Inspector General's regularly scheduled meetings with them and through other forums.

- ❖ Submitted our fiscal year 2008 budget request totaling \$26.8 million to the Office of Management and Budget in November 2006 and to cognizant congressional committees in February 2007. We shared these and related documents with senior corporate officials.

- ❖ Held quarterly meetings with FDIC Directors and other senior officials to keep them apprised of ongoing audit and evaluation reviews and results.

- ❖ Kept DSC, DRR, Legal, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This is accomplished by issuing e-mails to FDIC program offices on recent actions in OIG cases and OI's quarterly reports to DSC, DRR, Legal, and the Chairman's Office outlining activity and results in our cases involving closed and open banks, and asset and debt cases.

- ❖ Participated at Audit Committee meetings and presented results of significant assignments for consideration by Committee members.

- ❖ Identified the following management and performance challenges facing the Corporation and provided a detailed write-up of the challenges for inclusion in the Corporation's Performance and Accountability Report: addressing risks in large banks; maintaining strong regulatory capital standards; implementing deposit insurance reform; maintaining an effective examination and supervision program; granting insurance to and supervising



industrial loan companies; guarding against financial crimes in insured institutions; safeguarding the privacy of consumer information; promoting fairness and inclusion in the delivery of information, products, and services to consumers and communities; ensuring compliance with consumer protection laws and regulations and follow-up on violations; being ready for potential institution failures; and promoting sound governance and managing and protecting human, financial, information technology, physical, and procurement resources. We continue to work cooperatively with stakeholders to address these challenges.

- ❖ Participated with other OIGs in the President's Council on Integrity and Efficiency (PCIE), including attending monthly PCIE meetings and participating in PCIE Audit and Inspection & Evaluation Committee meetings.

- ❖ Met with representatives of the OIGs of the federal banking regulators (Federal Reserve Board, Department of the Treasury, National Credit Union Administration, Securities and Exchange Commission, Farm Credit Administration, Commodity Futures Trading Commission, Federal Housing Finance Board) to discuss audit and investigative matters of mutual interest.

- ❖ Elected new members of the OIG's Employee Advisory Group in January 2007. The new Employee Advisory Group is comprised of three employees from OI, two employees from OA, and one employee each from OE and the Office of Management.

- ❖ Continued to post and/or update information on the FDIC OIG internet (www.fdicig.gov) and intranet sites to ensure transparency and accessibility to OIG products, including Semiannual Reports to the Congress, OIG 2007 Business Plan, audit and evaluation reports, and investigation-related press releases.

Ensure Quality and Efficiency of OIG Audits, Evaluations, Investigations, and Other Operations

- ❖ Commencing work to revise OA's Policy and Procedures Manual to address changes in the performance audit standards and any process changes deemed necessary as a result of an internal assignment management review and the external peer review results.

- ❖ Began review of the Government Accountability Office (GAO) 2007 revision of Government Auditing Standards and planned for training staff on the revisions.



The new standards will be effective for engagements beginning on or after January 1, 2008.


- ❖ Held an entrance conference with the Department of State OIG on February 21, 2007. That office will conduct a peer review of our audit operations. Field work is expected to begin in April.
- ❖ In accordance with PCIE quality standards, we completed a peer review of the Department of Justice OIG Office of Audit and issued a final report in February 2007.
- ❖ Completed an internal quality control review of OA assignments. OI completed internal reviews of the Electronic Crimes Unit, OIG's Hotline Operations, Special Inquiries and Oversight, and the Eastern Region. OI internal reviews of Western Regional Offices (Dallas and Chicago) are expected to be completed by the end of the fourth quarter of the fiscal year.
- ❖ Developed a project management tracking and reporting process for internal OIG projects. The milestone documents for projects are updated each week and are used to track the status and progress of the OIG's internal improvement projects.

Enhance Strategic and Annual Planning and Performance Measurement

- ❖ Met to kick off the fiscal year 2008/2009 business planning process. The discussion included a look back at the fiscal year 2007 planning process to determine what worked well and what could be improved.
- ❖ Continued to assess and monitor changes in risk conditions that affect OIG business practices, including coordinating Inspector General assurance to the Chairman on the adequacy of internal controls for calendar year 2006 and updating OIG Management Control Plans and Accountability Units for CY 2007.

Invest in Cost-Effective and Secure IT

- ❖ Determined that updating the IT Strategic Plan to guide OIG business decisions, priorities, and resource allocations for 2008-2010 would be an office-wide initiative. Members of the OIG IT Strategic Plan Working Group were selected, and a meeting is planned in May to generate ideas, goals, and expectations for the IT Strategic Plan.
- ❖ Coordinated extensively with DIT to install new dedicated servers for OIG operations. OIG staff are in



the process of migrating the OIG's systems to the OIG's new servers. STAR, Counsel Workflow, Bank Case, Hotline, OIGNet, and the Training System were moved during March. The remaining OIG systems and files including, IDS and Dashboard are scheduled to be moved in April.

- ❖ DIT formally began its Laptop Replacement Project in December 2006. The OIG will be represented on both the steering committee and working group of participating FDIC divisions and offices.

- ❖ Continued to coordinate with DIT to ensure the security of OIG information in the FDIC computer network infrastructure.

- ❖ Attended a March 6, 2007 FDIC-sponsored Gartner Group presentation on planning and implementing Microsoft's new Vista and Office 2007 software.

- ❖ Attended a March 2007 meeting focused on the FDIC's enterprise architecture vision.

- ❖ Took steps to identify and evaluate the options and requirements needed to streamline, enhance, and improve the collection and reporting of information needed to manage OIG audits and evaluations. Current information systems and automated

tools will be evaluated and analyzed according to OIG management's information requirements to determine an optimal approach to meeting those requirements in a cost-effective and timely manner. A particular focus is on minimizing data entry, providing graphical representations of information, improving performance, and providing information across OIG systems and applications.

- ❖ Implemented the Training System upgrade in December 2006. The upgrade improved and streamlined the process of requesting and approving training for OIG professional, supervisory, and administrative staff using the system. The upgrade also provides features and improvements that make the process of obtaining vendor discounts and monitoring continuing professional education requirements more efficient.

- ❖ Updated the OIG Strategic Information Dashboard to incorporate the OIG fiscal year 2007 Business Plan strategic goals, performance goals, and key efforts. We also updated the quantitative measures and targets section that reports out on fiscal year 2007 performance targets as highlighted in the plan.

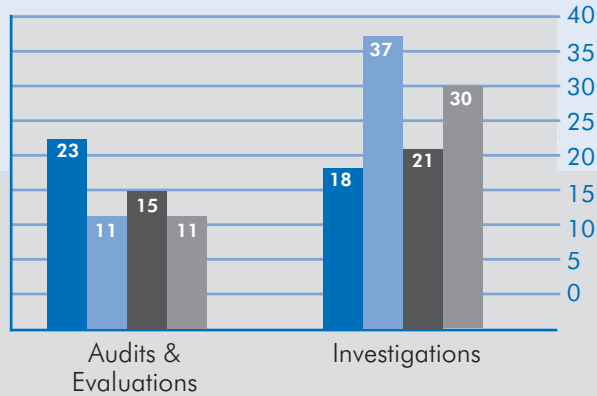
Cumulative Results (2-year period)

| Nonmonetary Recommendations | |
|-----------------------------|----|
| April 2005 - September 2005 | 39 |
| October 2005 - March 2006 | 34 |
| April 2006 - September 2006 | 48 |
| October 2006 - March 2007 | 35 |

LEGEND

- Apr 05 - Sept 05
- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07

Products Issued and Investigations Closed



LEGEND

- Apr 05 - Sept 05
- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07

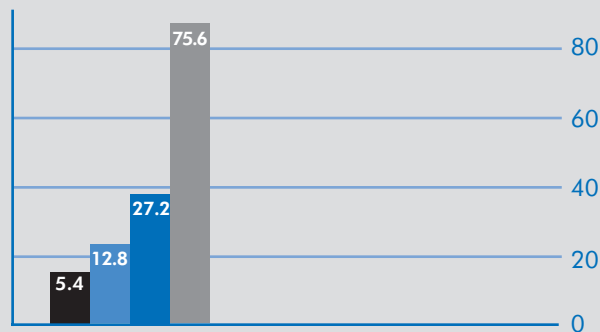
Questioned Costs/Funds Put to Better Use (in millions)



LEGEND

- Apr 05 - Sept 05
- Oct 05 - Mar 06
- Apr 06 - Sept 06
- Oct 06 - Mar 07

Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations (in millions)



Reporting Requirements

| Index of Reporting Requirements - Inspector General Act of 1978, as amended | |
|--|-------------|
| Reporting Requirements | Page |
| Section 4(a)(2): Review of legislation and regulations | 59 |
| Section 5(a)(1): Significant problems, abuses, and deficiencies | 11-50 |
| Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies | 11-50 |
| Section 5(a)(3): Recommendations described in previous semiannual reports on which corrective action has not been completed | 60 |
| Section 5(a)(4): Matters referred to prosecutive authorities | 10 |
| Section 5(a)(5) and 6(b)(2): Summary of instances where requested information was refused | 64 |
| Section 5(a)(6): Listing of audit reports | 62 |
| Section 5(a)(7): Summary of particularly significant reports | 11-50 |
| Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs | 63 |
| Section 5(a)(9): Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use | 64 |
| Section 5(a)(10): Audit recommendations more than 6 months old for which no management decision has been made | 64 |
| Section 5(a)(11): Significant revised management decisions during the current reporting period | 64 |
| Section 5(a)(12): Significant management decisions with which the OIG disagreed | 64 |

Information Required by the Inspector General Act of 1978, as amended

Review of Legislation and Regulations

The FDIC Office of Inspector General is tasked under the Inspector General Act of 1978 with reviewing existing and proposed legislation and regulations relating to programs and operations of the Corporation and making recommendations in the semiannual reports required by section 5(a) concerning the impact of such legislation or regulations on the economy and efficiency in the administration of programs and operations administered or financed by the Corporation or the prevention and detection of fraud and abuse in its programs and operations. The Office of Counsel reviewed legislative developments regarding H.R. 985, Whistleblower Protection Enhancements Act of 2007; H.R. 1300, the Program for Real Energy Security Act (PROGRESS Act); S. 495, the Data Privacy and Security Act of 2007 and updates to the Privacy Act. Additionally, Counsel's Office reviewed twelve FDIC directives related to reasonable accommodation, leave, community service, records management, Section 508 compliance, equal employment opportunity, worker's compensation, emergency preparedness, student educational employment program, and protecting sensitive information, and made comments on various aspects of these directives.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

This table shows the corrective actions management has agreed to implement but has not completed, along with associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in the audit reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by FDIC's Office of Enterprise Risk Management (OERM) and (2) the OIG's determination of closed recommendations for reports issued after March 31, 2002. These 15 recommendations from 13 reports involve improvements in operations and programs. OERM has categorized the status of these recommendations as follows:

Management Action in Process: (15 recommendations from 13 reports)

Management is in the process of implementing the corrective action plan, which may include modifications to policies, procedures, systems, or controls; issues involving monetary collection; and settlement negotiations in process.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

| Report Number, Title & Date | Significant Recommendation Number | Brief Summary of Planned Corrective Actions and Associated Monetary Amounts |
|---|-----------------------------------|---|
| Management Action In Process | | |
| 04-019 Enhancements to the FDIC System Development Life Cycle Methodology April 30, 2004 | 3 | Align systems development with the FDIC's Enterprise Architecture, establish how funding will be reviewed and provided in an iterative development environment, and update cost-benefit analysis during the life cycle of the system. |
| 05-016 Security Controls Over the FDIC's Electronic Mail (E-Mail) Infrastructure March 31, 2005 | 1● | Ensure that division and office directors provide FDIC employees and contractors with sufficiently detailed guidance to facilitate informed decisions on when to encrypt sensitive e-mail communications. |
| EVAL-06-005 FDIC Safeguards Over Personal Employee Information January 6, 2006 | 1 | Develop and issue an overarching privacy policy for safeguarding personal employee information. |
| 06-008 Consideration of Safety and Soundness Examination Results and Other Relevant Information in the FDIC's Risk-Related Premium System February 17, 2006 | 4◆ | Establish a schedule for periodically updating the assessment rate analysis and reassessing the basis point spreads and assessment rates, as needed. |
| 06-009 FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and Fair and Accurate Credit Transactions (FACT) Act February 24, 2006 | 2* | Develop, in coordination with the joint-agency rulemaking committee, a more aggressive project management plan that will expedite the issuance of final rules and regulations for all FACT Act provisions. |
| 06-011 Challenges and FDIC Efforts Related to Predatory Lending June 7, 2006 | 2◆ | Review existing examiner, financial institution, and consumer guidance and determine whether additional guidance is needed to address the risks associated with predatory lending. |

- Management has taken actions to address this recommendation. The OIG plans to assess the effectiveness of those actions as part of the OIG's 2007 work under the Federal Information Security Management Act and will then determine whether the recommendation can be closed.
- ◆ The OIG has received some information but has requested additional information to evaluate management's actions in response to the recommendation.
- * The OIG has not yet evaluated management's actions in response to the OIG recommendation.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed (cont.)

| Report Number, Title & Date | Significant Recommendation Number | Brief Summary of Planned Corrective Actions and Associated Monetary Amounts |
|---|-----------------------------------|--|
| 06-013 FDIC Reserve Ratio and Assessment Determinations April 17, 2006 | 2 | Review the existing Corporate Bylaws to ensure that those delegations reflect the Board members' intent and expectations with regard to the deposit insurance fund reserve ratio and assessment determination processes. |
| | 3 | Work with FDIC management to evaluate procedures and practices for keeping Board members informed of Corporation matters and activities. |
| 06-014 FDIC's Industrial Loan Company Deposit Insurance Application Process July 20, 2006 | 2 | Develop and issue clarifying policy or guidance regarding the need for, and importance of, conditions associated with deposit insurance applications. |
| 06-015 FDIC's Oversight of Technology Service Providers (TSP) July 20, 2006 | 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. |
| 06-017 DRR's Protection of Bank Employee and Customer Personally Identifiable Information September 15, 2006 | 1 | Develop a DRR Records Management Program that includes guidelines for the inventory, maintenance, use, and control of hardcopy records containing personally identifiable information from failed institutions. |
| 06-024 Division of Supervision and Consumer Protection's Supervisory Actions Taken for Compliance Violations September 29, 2006 | 1 | Strengthen guidance related to the monitoring and follow-up processes for compliance violations by revising the Compliance Examination Procedures to require follow-up between examinations on repeat, significant compliance violations and program deficiencies. |
| 06-025 Controls for Monitoring Access to Sensitive Information Processed by FDIC Applications September 29, 2006 | 1 | Develop an enterprise-wide approach for monitoring user access privileges commensurate with the sensitivity of the FDIC's information systems and data. |
| | 3 | Develop a written plan that defines a risk-based, enterprise-wide approach to audit logging and monitoring for the FDIC's portfolio of information systems. |
| EVAL-06-026 FDIC's Contract Administration September 29, 2006 | 13 | Define requirements for the new automated procurement system, including to address the New Financial Environment shortcomings identified in this report. |

■ The OIG has not received information necessary to evaluate management's actions in response to the recommendation.

Table II: Audit Reports Issued by Subject Area

| Audit Report | | Questioned Costs | | Funds Put to Better Use |
|------------------------------|---|------------------|-------------|-------------------------|
| Number and Date | Title | Total | Unsupported | |
| Supervision | | | | |
| 07-001 December 14, 2006 | FDIC's Supervision of Financial Institutions' OFAC Compliance Programs | | | |
| 07-002 January 10, 2007 | Division of Supervision and Consumer Protection's Information Technology-Risk Management Program | | | |
| 07-007 March 30, 2007 | Examination Assessment of the Reliability of Appraisals and Sufficiency of Insurance Coverage for Real Estate Lending | | | |
| Consumer Protection | | | | |
| 07-005 February 5, 2007 | Information Technology Examination Coverage of Financial Institutions' Oversight of Technology Service Providers | | | |
| 07-008 March 30, 2007 | FDIC's Implementation of the 2005 Amendments to the Community Reinvestment Act Regulations | | | |
| Resources Management | | | | |
| 07-003 January 10, 2007 | FDIC's Compliance with Section 522 of the Consolidated Appropriations Act, 2005 | | | |
| 07-004 January 10, 2007 | Interagency Agreement with the General Services Administration for the Infrastructure Services Contract | | | |
| 07-006 March 28, 2007 | Management Report: Independent Evaluation of the FDIC's Information Security Program - 2006 | | | |
| 07-009 March 30, 2007 | FDIC's Contract Planning and Management for Business Continuity | | | |
| Totals for the Period | | \$0 | \$0 | \$0 |

Table III: Evaluation Reports Issued

| Number and Date | Title |
|-------------------------------|---|
| EVAL-07-001 March 28, 2007 | FDIC's Succession Planning Efforts |
| EM-07-001 March 30, 2007 | FDIC's Management Report Information Flow |

Table IV: Audit Reports Issued with Questioned Costs

| | Number | Questioned Costs | |
|--|----------|------------------|-------------|
| | | Total | Unsupported |
| A. For which no management decision has been made by the commencement of the reporting period. | 0 | 0 | 0 |
| B. Which were issued during the reporting period. | 0 | 0 | 0 |
| Subtotals of A & B | 0 | \$0 | \$0 |
| C. For which a management decision was made during the reporting period. | 0 | 0 | 0 |
| (i) dollar value of disallowed costs. | 0 | 0 | 0 |
| (ii) dollar value of costs not disallowed. | 0 | 0 | 0 |
| D. For which no management decision has been made by the end of the reporting period. | 0 | 0 | 0 |
| Reports for which no management decision was made within 6 months of issuance. | 0 | 0 | 0 |

Table V: Audit Reports Issued with Recommendations for Better Use of Funds

| | Number | Dollar Value |
|--|----------|--------------|
| A. For which no management decision has been made by the commencement of the reporting period. | 0 | 0 |
| B. Which were issued during the reporting period. | 0 | 0 |
| Subtotals of A & B | 0 | \$0 |
| C. For which a management decision was made during the reporting period. | 0 | 0 |
| (i) dollar value of recommendations that were agreed to by management. | 0 | 0 |
| - based on proposed management action. | 0 | 0 |
| - based on proposed legislative action. | 0 | 0 |
| (ii) dollar value of recommendations that were not agreed to by management. | 0 | 0 |
| D. For which no management decision has been made by the end of the reporting period. | 0 | 0 |
| Reports for which no management decision was made within 6 months of issuance. | 0 | 0 |

Table VI: Status of OIG Recommendations Without Management Decisions

During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VII: Significant Revised Management Decisions

During this reporting period, there were no significant revised management decisions.

Table VIII: Significant Management Decisions with Which the OIG Disagreed

During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table IX: Instances Where Information Was Refused

During this reporting period, there were no instances where information was refused.

Congratulations to OIG Retirees



Marilyn Kraus

Marilyn Kraus retired in April 2007. Her distinguished career of federal service began in May 1971 as a summer hire at the Cameron Station Post Exchange then progressed to service for the Interstate Commerce Commission, the General Services Administration, Federal Home Loan Bank Board, and finally, the FDIC. Beginning in 1987, she held a number of positions with the FDIC OIG, including at the audit manager and director level. Her service closely paralleled significant events in the FDIC's history. Her work involving FDIC resolution and receivership activities for failed financial institutions was part of our nation's response to the challenges posed by that crisis. As the risks posed by the crisis subsided, the FDIC entered a period of internal transformation, and her work as the Director for Resources Management Audits helped ensure that the FDIC adopted sound business practices and carefully considered the efficiency and effectiveness of its operations. Work conducted just prior to her retirement involving business continuity planning will have a long-term, positive impact on the FDIC's ability to respond to emergency situations.



Rex Simmons

Rex Simmons, Assistant Inspector General for Management and Congressional Relations, retired after more than 32 years of public service. His career included work for the National Park Service in North Carolina, the U.S. Government Accountability Office (GAO), the Resolution Trust Corporation (RTC), and finally, the FDIC OIG. At the GAO, over a period of 15 years, he excelled as an auditor and evaluator, and contributed to the success of a variety of government programs and operations. When the RTC was created in 1989 to handle the savings and loan crisis, he played a key role in establishing and developing the Office of Inspector General as part of the executive team. He helped ensure that RTC headquarters and regional sites operated in the true spirit of an Office of Inspector General: effectively, efficiently, and economically. He was also instrumental in the successful merger of the RTC and the FDIC following the RTC's sunset in 1995. Since the merger he led his staff in providing outstanding business support for the FDIC OIG in the areas of budget, human resources, and information technology; strategic planning and performance measurement; policy development and review; and congressional relations.



The Office of Inspector General (OIG) Hotline is a convenient mechanism employees, contractors, and others can use to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations. The OIG maintains a toll-free, nationwide Hotline (1-800-964-FDIC), electronic mail address (IGHotline@FDIC.gov), and postal mailing address. The Hotline is designed to make it easy for employees and contractors to join with the OIG in its efforts to prevent fraud, waste, abuse, and mismanagement that could threaten the success of FDIC programs or operations.

To learn more about the FDIC OIG and for complete copies of audit and evaluation reports discussed in this Semiannual Report, visit our Web site: <http://www.fdicig.gov>

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226