



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 homepage: <http://www.fdicig.gov>

Federal Deposit Insurance Corporation
Office of Inspector General
801 17th St., NW Washington, D.C. 20434



SEMIANNUAL REPORT TO THE
CONGRESS

April 1, 2005 – September 30, 2005

OFFICE OF INSPECTOR GENERAL
FEDERAL DEPOSIT INSURANCE CORPORATION

Hurricane Relief Fraud Hotline

If you have knowledge of fraud, waste, abuse, or allegations of mismanagement involving hurricane relief operations, you can:

- Call the Hurricane Relief Fraud Hotline at (866) 720-5721
- Fax the Hurricane Relief Fraud Hotline at (703) 604-8567
- Email: katrinafraud@dodig.mil
- Or write: Hurricane Relief Hotline
Washington, D.C. 20301-1900

*Calls can be made anonymously
and confidentially*

Congratulations!

The OIG congratulates all award recipients!

OIG Staff Receive PCIE Awards for Excellence

The evaluation team of Marshall Gentry, Ann Lewis, Loretta Weibel, Steve Beard, and Adriana Vosburg received an award for their outstanding work on the complex evaluation of the FDIC's approach for supervising limited-charter depository institutions.



L to R: Stephen Beard, Ann Lewis, Marshall Gentry, Loretta Weibel, and Russell Rau. Not pictured - Adriana Vosburg.

The audit team of Michael Lombardi, Joyce Cooper, Rhoda Allen, DeGloria Hallman, Philip Hodge, Jeffery Smullen, Larry Jones, Diana Chatfield, Steve Beard, and Adriana Vosburg received an award for their outstanding work on the congressionally requested audit of the FDIC's supervision of a financial institution's compliance with the Bank Secrecy Act.



L to R: Stephen Beard, Philip Hodge, DeGloria Hallman, Diana Chatfield, Joyce Cooper, Mike Lombardi, and Russell Rau. Not pictured - Rhoda Allen, Adriana Vosburg, Jeffery Smullen, and Larry Jones.



Sharon Tushin received a PCIE Award for Excellence, along with other members of the Inspector General E-Learning Steering Committee, for their groundbreaking efforts in launching the SkillSoft

pilot e-learning program for the federal Inspector General community.



The OIG Congratulates Former Inspector General Gaston L. Gianni, Jr.

In recognition of Gaston's contributions to the Inspector General community and his lifelong commitment to efficient and effective government,

the PCIE has renamed one of its most prestigious awards in his honor. The *Gaston L. Gianni, Jr. Better Government Award* will be given annually to recognize persons who contribute to attaining the ideals of the Inspector General Act and work to improve the public's confidence in government.



SEMIANNUAL REPORT TO THE
CONGRESS
April 1, 2005–September 30, 2005

OFFICE OF INSPECTOR GENERAL
FEDERAL DEPOSIT INSURANCE CORPORATION



Contents

Inspector General’s Statement.....	1
Overview	3
Highlights.....	5
Management and Performance Challenges	7
Investigations: Making an Impact.....	25
OIG Organization: Pursuing OIG Goals	41
Fiscal Year 2005 Performance Report Summary	49
Reporting Requirements.....	51
Reader’s Guide to Inspector General Act Reporting Terms	52
Statistical Information Required by the Inspector General Act of 1978, as amended.....	54
Farewell to OIG Retirees.....	60
Abbreviations and Acronyms	62
Tables	
Table 1: Significant OIG Achievements.....	47
Table 2: Nonmonetary Recommendations.....	47
Figures	
Figure 1: FDIC Security Assurance Trend Analysis.....	11
Figure 2: Office of Investigations Case Distribution.....	26
Figure 3: Products Issued and Investigations Closed.....	47
Figure 4: Questioned Costs/Funds Put to Better Use.....	48
Figure 5: Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations.....	48





Inspector General's Statement

The past semiannual reporting period has been marked by significant organizational change in the Office of Inspector General (OIG). Three members of our senior management team retired, and several reorganizations, planned office closings, and changes in leadership responsibilities have been announced. Other OIG staff retired or left to pursue different opportunities, and through a buyout program offered by the OIG, six additional members of the OIG will be leaving our office at the end of the calendar year. Thus, our staff has been adjusting to a significantly different working environment, and I am proud of their continued focus on the OIG mission and impressive results during this time of flux.

To illustrate, during the reporting period, we achieved great success with a significant case involving a failed institution—BestBank. A Denver jury returned guilty verdicts on 63 counts—bank fraud, operating a continuing financial crimes enterprise, making false bank reports, and wire fraud—against two people involved in a complex financial institution and consumer fraud that led to the 1998 failure of BestBank and concomitant \$200 million loss to the Bank Insurance Fund. We have been working with the Department of Justice, the Federal Bureau of Investigation, and the Internal Revenue

Service on the case since that time. Given the losses to the fund, consumers, and uninsured depositors, as well as the message the convictions send about the government's refusal to tolerate such criminal activity, it was a worthy investment.

On the audit side, we conducted extensive work and issued three products to satisfy our Federal Information Security Management Act reporting responsibilities. We reported that the FDIC has made significant progress in improving its information security controls and practices and additional improvements were underway at the time of our evaluation. We identified no significant deficiencies as defined by the Office of Management and Budget that warranted consideration as a potential material weakness. We identified seven steps that the Corporation can take to enhance its information security program and practices, and we continue to coordinate closely with FDIC management on corporate information security efforts.

From an overall OIG perspective, and as summarized in the Organization section of this semiannual report, we completed our Fiscal Year 2005 Performance Report, which measures our progress in achieving 37 goals. These goals emphasize (1) adding value by achieving impact on issues of importance to the Corpo-

ration and our other stakeholders; (2) fostering effective communications with our stakeholders; (3) aligning human resources to support the OIG mission; and (4) managing our resources effectively. We met or substantially met 31, or 84 percent, of the 37 goals. We also completed our seventh client survey to solicit views of corporate management on the products and processes of our office. Both of these initiatives are helping to guide us as we pursue a new approach to planning the future direction and strategic focus of our office.

In connection with the changing environment of the OIG, I must also mention the many changes that the Corporation as a whole has experienced over the past months, particularly in its governance structure. Former Vice Chairman John Reich is now the Director of the Office of Thrift Supervision and in that new capacity continues to be a member of the FDIC Board, along with newly appointed Director John Dugan, the Comptroller of the Currency. Martin Gruenberg assumed his position as Vice Chairman of the FDIC in August 2005, and it has been a pleasure to work with him, particularly in his new role as Chairman of the FDIC Audit Committee. I look forward to continued coordination with him and other senior leadership of the FDIC as we all seek to ensure stability and public confidence in the nation's financial system.

Finally, a disastrous event occurred in early September that could have undermined that very stability and public confidence in the Gulf Coast region—Hurricane Katrina. The FDIC responded promptly by establishing a

center staffed 24 hours a day, 7 days a week, by FDIC volunteers. The goal was to assist bank customers with a wide range of problems, such as how to access their accounts, and to gather and convey information regarding the operations of affected institutions. A number of other initiatives to help bankers through the hurricane's aftermath are underway. Significantly, as we were going to press, after more than 4 years with the FDIC, Chairman Donald Powell was named by the President to serve as the federal coordinator for long-term hurricane recovery efforts and will soon be leaving the Corporation. We wish him well in this critical endeavor.

The OIG also took a number of actions in response to the hurricane, including participating in the Department of Justice Hurricane Katrina Fraud Task Force, communicating with other federal Inspectors General about the governmentwide response to the storm, creating a Web page for financial institutions and consumers to report instances of fraud, providing volunteer resources in support of the Center for Missing and Exploited Children, and meeting with audit representatives from other financial regulatory OIGs to coordinate possible future work related to relief and rebuilding activities. I appreciate the commitment and concern of all OIG staff who have stepped up to help. In the true spirit of public service, we will continue to monitor the impact of Katrina on the financial services industry and do whatever we can to assist fellow citizens in the aftermath of this tragedy.



Patricia M. Black
Deputy Inspector General
October 31, 2005



Overview

Management and Performance Challenges

The Management and Performance Challenges section of our report presents OIG results of audits, evaluations, and other reviews carried out during the reporting period in the context of the OIG's view of the most significant management and performance challenges facing the Corporation. We identified the following seven management and performance challenges and, in the spirit of the Reports Consolidation Act of 2000, we presented our assessment of them to the Chief Financial Officer of the FDIC in December 2004. The Act calls for these challenges to be presented in the FDIC's consolidated performance and accountability report. The FDIC includes such reporting as part of its Annual Report. Our work has been and continues to be largely designed to address these challenges and thereby help ensure the FDIC's successful accomplishment of its mission.

- Corporate Governance in Insured Depository Institutions
- Management and Analysis of Risks to the Insurance Funds
- Security Management

- Money Laundering and Terrorist Financing
- Protection of Consumer Interests
- Corporate Governance in the FDIC
- Resolution and Receivership Activities

OIG work conducted to address these areas during the current reporting period includes 23 audit and evaluation reviews containing questioned costs of \$981,355 and 39 non-monetary recommendations; investigations addressing a number of the areas of challenge; comments and input to the Corporation's draft policies in significant operational areas; participation at meetings, symposia, conferences, and other forums to jointly address issues of concern to the Corporation and the OIG; and other assistance provided to the Corporation. (See pages 7-24.)

Investigations: Making an Impact

In the Investigations section of our report, we feature the results of work performed by OIG agents in Washington, D.C.; Atlanta; Dallas; and Chicago. OIG agents conduct investigations of alleged criminal or otherwise prohibited activities impacting the

FDIC and its programs. In conducting investigations, the OIG works closely with U.S. Attorneys' Offices throughout the country in attempting to bring to justice individuals who have defrauded the FDIC. The legal skills and outstanding direction provided by Assistant United States Attorneys with whom we work are critical to our success. The results we are reporting for the last 6 months reflect the efforts of U.S. Attorneys' Offices throughout the United States. Our write-ups also reflect our partnering with the Federal Bureau of Investigation, the Internal Revenue Service, and other law enforcement agencies in conducting investigations of joint interest. Additionally, we acknowledge the invaluable assistance of the FDIC's Divisions and Offices with whom we work closely to bring about successful investigations.

Investigative work during the period led to indictments or criminal charges against 22 individuals and convictions of 19 defendants. Criminal charges remained pending against 34 individuals as of the end of the reporting period. Fines, restitutions, and recoveries resulting from our cases totaled approximately \$5.4 million. This section of our report also includes a brief update on the work of our Electronic Crimes Unit and cites acknowledgements given to several of our Special Agents and to others with whom we work. (See pages 25-40.)

OIG Organization: Pursuing OIG Goals

In the Organization section of our report, we note some of the significant internal activities that the FDIC OIG has pursued during the past 6 months in furtherance of our four strategic goals and corresponding objectives. These activities complement and support the audit, evaluation, and investigative work discussed in the earlier sections of our report. Activities of OIG Counsel and cumulative OIG results covering the past five reporting periods are also shown in this section. In the interest of transparency and accountability, we are also providing a sum-

mary of our Fiscal Year 2005 Performance Report. (See pages 41-50.)

Statistical Information

The Appendix of our report contains much of the statistical information required under the Inspector General Act, as amended. (See pages 54-59.)

Other Material

We bid farewell to retired OIG staff members whose contributions to our office are very much appreciated. We also provide a listing of abbreviations and acronyms. Finally, we congratulate 2005 President's Council on Integrity and Efficiency Award Winners. (See pages 60-end.)



Highlights

- The Office of Audits issues 23 reports containing total questioned costs of \$981,355 and 39 nonmonetary recommendations to improve corporate operations and activities. Among these are recommendations to strengthen the compliance examination process, enhance the central data repository project management, and strengthen controls related to FDIC employee travel.
- OIG investigations result in 22 indictments/informations; 19 convictions; and approximately \$5.4 million in total fines, restitution, and other monetary recoveries.
- OIG Counsel provides advice and counsel to OIG staff on a number of issues, including applicability of privacy-related laws and regulations to the FDIC, and banking law matters related to compliance examinations and corrective and enforcement actions. Counsel is involved in 28 litigation matters, 3 of which were resolved during the reporting period and the remainder of which are awaiting further action.
- The OIG reviews and comments on 3 proposed formal regulations, 1 legislative proposal—the Personal Data Privacy and Security Act of 2005, 16 proposed FDIC policies and directives, and responds to 4 requests under the Freedom of Information Act. Substantive comments are provided to the Corporation related to proposed policies on various aspects of information technology security risk management and the risk-related premium system.
- The OIG completes its fifth FDIC information security evaluation, noting the Corporation's significant progress in strengthening security controls and practices.
- The OIG coordinates with and assists management on a number of initiatives, including Office of Investigations and Office of Audits Executives' participation at Division and Office meetings, administration of the OIG's seventh client survey, and presentations as part of the Corporate Employee Program.
- The OIG announces and implements downsizing and reorganization initiatives and takes step to enhance officewide strategic planning efforts.
- The OIG accomplishes a number of internal office initiatives, including establishing a mentoring program, actively participating in e-learning opportunities,

and participating in numerous inter-agency working groups and roundtables through the President's Council on Integrity and Efficiency.

- OIG Special Agent is acknowledged by the U.S. Attorney's Office, District of Connecticut, for exemplary work in a joint investigation with the Federal Bureau of Investigation and the Internal Revenue Service Criminal Investigation Division in the prosecution of the former Chairman of the Board of Directors of Connecticut Bank of Commerce.
- The OIG issues its Fiscal Year 2005 Performance Report wherein we report that we met or substantially met 84 percent of our performance goals.
- The OIG coordinates with corporate management to address an incident involving unauthorized release of FDIC employee data and meets with congressional staff to discuss the matter. The OIG initiates several assignments related to protection of personal information – both internal to the FDIC and with respect to the institutions it supervises.
- The OIG formulates the audit and evaluation assignment plan for fiscal year 2005 and consults and coordinates with FDIC management and congressional staff in doing so.



Management and Performance Challenges

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 4,545 individuals within seven specialized operating divisions and other offices carry out the FDIC mission throughout the country. According to most current data in the Corporation's Letter to Stakeholders, issued for the 3rd Quarter 2005, the FDIC insured \$3.757 trillion in deposits for 8,881 institutions, of which the FDIC supervised 5,257. The Corporation held insurance funds of \$48 billion to ensure depositors are safeguarded. The FDIC had \$475 million in assets in liquidation in 28 Bank Insurance Fund and Savings Association Insurance Fund receiverships.

In the spirit of the Reports Consolidation Act of 2000, and to provide useful perspective for readers, we present a large body of our work in the context of "the most significant management and performance challenges" facing the Corporation. The Act calls for these challenges to be included in the consolidated performance and accountability reports of those federal agencies to which it applies.

In December 2004, we updated our assessment of these challenges and provided them to the Corporation. The 7 challenges we have identified are listed below. In the past several years, we identified 10 challenges. As part of our December 2004 assessment, we consolidated a number of the challenges into "Corporate Governance in the FDIC" and introduced "Money Laundering and Terrorist Financing" as a new challenge.

The Corporation has a number of actions underway to address many of the issues discussed below, and we encourage continued attention to each challenge. We will continue to conduct audits, evaluations, investigations, and other reviews related to these challenges and look forward to continuing to work cooperatively with the Corporation as we do so.

We identified the following challenges, and the Corporation included them in its 2004 Annual Report:

1. Corporate Governance in Insured Depository Institutions
2. Management and Analysis of Risks to the Insurance Funds
3. Security Management
4. Money Laundering and Terrorist Financing
5. Protection of Consumers' Interests
6. Corporate Governance in the FDIC
7. Resolution and Receivership Activities

Corporate Governance in Insured Depository Institutions

Corporate governance is generally defined as the fulfillment of the broad stewardship responsibilities entrusted to the Board of Directors, officers, and external and internal auditors of a corporation. A number of well-publicized announcements of business and accountability failings, including those of financial institutions, have raised questions about the credibility of management oversight and accounting practices in the United States. In certain cases, board members and senior management engaged in high-risk activities without proper risk management processes, did not maintain adequate loan policies and procedures, and circumvented or disregarded various laws and banking regulations. In an increasingly consolidated financial industry, effective corporate governance is needed to ensure adequate stress testing and risk management processes covering the entire organization. Adequate corporate governance protects the depositor, institution, nation's financial system, and FDIC in its role as deposit insurer. A lapse in corporate governance can lead to a rapid decline in public confidence, with potentially disastrous results to the institution.

With respect to financial institutions, in some cases, dominant officials have exercised undue control over operations to the institution's detriment. In other cases, independent public accounting firms rendered clean opinions on the institutions' financial statements when, in fact, the statements were materially misstated. Such events have increased public concern regarding the adequacy of corporate governance and, in part, prompted passage of the Sarbanes-Oxley Act of 2002. This Act has focused increased attention on management assessments of internal controls over financial reporting and the external auditor attestations of these assessments. Strong stewardship along with reliable financial reports from insured depository institutions are critical to FDIC mission achievement.

The FDIC has initiated various measures designed to mitigate risks posed by these concerns, such as reviewing the bank's board activities and ethics policies and practices and reviewing auditor independence requirements. In fact, many of the Sarbanes-Oxley Act requirements parallel those already applicable to the FDIC under the FDIC Improvement Act. The FDIC also reviews the publicly traded companies' compliance with Securities and Exchange Commission regulations and the approved and recommended policies of the Federal Financial Institutions Examination Council to help ensure accurate and reliable financial reporting through an effective external auditing program and on-site FDIC examination.

Our investigative work is one way of addressing corporate governance issues. In a number of cases, financial institution fraud is a principal contributing factor to an institution's failure. Unfortunately, the principals of some of these institutions—that is, those most expected to ensure safe and sound corporate governance—are at times the parties perpetrating the fraud. Our Office of Investigations plays a critical role in addressing such activity. (See the Investigations section of this report for specific examples of bank fraud cases involving corporate governance weaknesses.)

Management and Analysis of Risks to the Insurance Funds

A primary goal of the FDIC under its insurance program is to ensure that its deposit insurance funds do not require augmentation by the U.S. Treasury. Achieving this goal is a challenge that requires effective communication and coordination with the other federal banking agencies. The FDIC engages in an ongoing process of proactively identifying risks to the deposit insurance funds and adjusting the risk-based deposit insurance premiums charged to the institutions. The consolidations that have occurred among banks, securities firms, insurance companies, and other financial services providers resulting from the Gramm-Leach-Bliley Act involve increasingly diversified activities and associated inherent risks.

In some instances, bank mergers have created “large banks,” which are generally defined as institutions with assets of over \$25 billion. As of June 30, 2005 the 25 largest banks controlled \$5.64 trillion (54 percent) of total bank assets in the country. The FDIC is the primary federal regulator for only 2 of these 25 institutions.

To address the risks associated with large banks for which the FDIC is the insurer but is not the primary federal regulator, the FDIC has established the Large Bank Section in the Division of Supervision and Consumer Protection (DSC). A key effort is the Dedicated Examiner Program for the largest banks in the United States. One senior examiner from the FDIC is dedicated to each institution and participates in targeted reviews or attends management meetings. Additionally, case managers closely monitor such institutions through the Large Insured Depository Institutions Program’s quarterly analysis and executive summaries and consistently remain in communication with their counterparts at the other regulatory agencies.

For large banks, under Basel II, capital will be determined by the banks’ internal estimates of risk. The FDIC and other regulators are

evaluating policy options to ensure that institutions and the industry as a whole maintain adequate capital and reserves. Meanwhile, the FDIC and other regulators must work to ensure that they have staff with necessary expertise to understand and evaluate the adequacy of the institutions’ capital models.

Another area of challenge for the Corporation relates to industrial loan companies (ILCs). The FDIC is the primary federal regulator for a number of ILCs, which are insured depository institutions owned by organizations that are subject to varying degrees of federal regulation. ILC charters allow mixing of banking and commerce which is otherwise prohibited for most other depository institutions owned by commercial firms.

Finally, there has been ongoing congressional consideration to merging the Bank Insurance Fund (BIF) and Savings Association Insurance Fund (SAIF) in the hope that the merged fund would not only be stronger and better diversified but would also eliminate the concern about a deposit insurance premium disparity between the BIF and the SAIF. Assessments in the merged fund would be based on the risk that institutions pose to that fund. The prospect of different premium rates for identical deposit insurance coverage would be eliminated. The Corporation has worked hard to bring about deposit insurance reform and, as of the end of the reporting period, was expecting Congressional action in this regard.

Our work in this area included the following three audits.

MERIT Eligibility Process

The FDIC’s DSC is responsible for conducting streamlined safety and soundness examinations under the Maximum Efficiency, Risk-focused, Institution Targeted (MERIT) examination guidelines. Under MERIT, an FDIC Examiner-in-Charge determines the eligibility of an institution for a safety and

soundness examination under MERIT guidelines during the pre-examination planning phase by applying MERIT eligibility criteria to the FDIC's knowledge of an institution, its size, complexity, and risk profile. To place this program in perspective, from May 1, 2002, through September 30, 2004, the FDIC conducted 2,290 MERIT examinations.

During the reporting period, we conducted an audit to determine whether the FDIC's process for determining an institution's eligibility for an examination under MERIT guidelines adequately considered the appropriate risk factors, and we concluded that it did. The MERIT eligibility criteria include a range of appropriate banking risk indicators that should identify those institutions with a higher risk profile that do not qualify for a streamlined examination. Also, about 18 months after launching this streamlined examination program, the FDIC conducted an evaluation of the MERIT guidelines that resulted in expanding, strengthening, and revising the MERIT eligibility criteria. Further, for the examinations we reviewed, examiners adequately applied the FDIC's MERIT eligibility criteria and screening process performed during pre-examination planning to provide reasonable assurance that only low-risk institutions qualified for a MERIT examination.

However, we found that the 33 pre-examination planning memoranda we reviewed did not always clearly reflect the decisions made about an institution's MERIT eligibility. In our view, additional information reflecting the MERIT eligibility decision would increase assurance that the MERIT criteria are adequately considered and that examination procedures are planned commensurate with the relevant existing and potential risks at an institution. We therefore made two recommendations for updating and clarifying pre-examination planning guidance. FDIC management concurred with both of them.

Effectiveness of Supervisory Corrective Actions

The FDIC uses a number of tools to address supervisory concerns related to the safety and soundness of financial institutions and their compliance with laws and regulations. These tools range from informal advice and written agreements to formal actions that are legally enforceable. Supervisory corrective actions are tailored to each situation and address the specific problems at an institution.

We conducted an audit to determine whether supervisory corrective actions taken against FDIC-supervised institutions achieved the intended purposes before being terminated. Our audit focused on the FDIC's use of Cease and Desist orders and Memorandums of Understanding – two of the more commonly used supervisory corrective actions. We found that sufficient controls are in place and operating effectively to ensure that supervisory corrective actions achieve their intended purposes before being terminated.

We also found that DSC could improve the timeliness and completeness of data in its Formal and Informal Action Tracking system (FIAT). Information for 14 of the 15 actions we reviewed often was not entered into the system in a timely or complete manner. In addition, the system did not include formal enforcement actions that state regulators independently issued to FDIC-supervised institutions. As a result, DSC cannot fully rely on the FIAT data and management reports for monitoring supervisory corrective actions.

Our report contains three recommendations intended to improve the timeliness and completeness of FIAT data. FDIC management agreed with the recommendations.

Capital Provisions Established Under Supervisory Corrective Actions

We conducted an audit to determine whether DSC's process is adequate for determining capital provision requirements established under supervisory corrective actions for problem banks.

We concluded that DSC has been successful in using capital provisions as part of overall supervisory actions to improve the financial structure of problem institutions, and its related processes are adequate. Also, examiners were analyzing capital adequacy and the bank's adherence to supervisory corrective action capital provisions in accordance with DSC policies. We also found, however, that supervisory personnel were not recommending capital provisions that encompass all of the Prompt Corrective Action (PCA) capital ratios. As a result, the established capital provisions did not ensure that banks stay adequately capitalized as defined by the PCA capital categories.

We recommended that DSC revise guidance to supervisory personnel regarding the use and consideration of PCA capital ratios in the formulation and recommendation of capital provision requirements. DSC generally concurred with the findings of the report and agreed to implement the recommendation.

Security Management

The FDIC relies heavily upon automated information systems to collect, process, and store vast amounts of banking information. This information is used by financial regulators, academia, and the public to assess market and institution conditions, develop regulatory policy, and conduct research and analysis on important banking issues. Ensuring the confidentiality, integrity, and availability of this information in an environment of increas-

ingly sophisticated security threats requires a strong, enterprise-wide information security program at the FDIC and insured depository institutions. It also requires compliance with applicable statutes and policies aimed at promoting information security throughout the federal government. One such statute is Title III of the E-Government Act of 2002, commonly referred to as the Federal Information Security Management Act of 2002 (FISMA). As a result of focused efforts over the past several years, and as illustrated in Figure 1, the FDIC has made significant progress in improving its information security controls and practices and addressing current and emerging information security requirements mandated by FISMA.

Also with respect to security management, the FDIC and insured depository institutions need to continue to ensure that sound disaster recovery and business continuity planning is present to safeguard depositors, investors, and others who depend on the financial services.

Figure 1: FDIC Security Assurance Trend Analysis



Source: Annual FDIC OIG evaluations of the FDIC's information security program. (Evaluations in 2001 and 2002 were done pursuant to legislation preceding FISMA. In 2003, we did more in-depth work in 3 areas, in response to new FISMA requirements.)

Federal Information Security Management Act

We issued three products to satisfy our FISMA reporting responsibilities: an Office of Management and Budget (OMB) Security Questions Report, a Privacy Information Report, and our comprehensive Security Evaluation Report with Scorecard. We reported that the FDIC has made significant progress in improving its information security controls and practices and additional improvements were underway at the time of our evaluation. We identified no significant deficiencies as defined by the OMB that warrant consideration as a potential material weakness. We did note, however, that management attention is needed in several key security control areas to ensure that appropriate risk-based and cost-effective security controls are in place to secure the FDIC's information resources and further the Corporation's security goals and objectives. Consequently, we concluded that the FDIC had established and implemented management controls that provided limited assurance over its information resources.

We identified steps that the Corporation can take to strengthen its information security program and practices. These related to: enhancing the FDIC's inventory of information systems and categorizing the systems based on impact levels; enhancing the information security risk management program; improving contractor oversight and the effectiveness of disaster recovery tests; and integrating security standards in the enterprise architecture and better integrating security processes.

The Corporation has begun to develop plans of action and milestones to address the actions we suggested.

Controls Over the Risk-Related Premium System

The Risk-Related Premium System (RRPS) is the FDIC's system of record for the risk assessment classification of financial institu-

tions. This system contains examination and supervisory action information that is considered highly sensitive and is not available to the public. The insurance premium assessed to each institution is based on the balance of assessable deposits held during the preceding two quarters and on the degree of risk the institution poses to the BIF or the SAIF. The FDIC uses a risk-based premium system that assesses higher rates on those institutions that pose greater risks to the insurance fund.

The RRPS calculates assessment rates based on data from such sources as the institutions' Call Reports; Thrift Financial Reports; examination data from the FDIC, Office of the Comptroller of the Currency, Federal Reserve Board, and Office of Thrift Supervision; and input from FDIC personnel. In an audit we conducted during the period, we wanted to determine whether the RRPS application provides the appropriate level of confidentiality, data integrity, and availability through the use of effective management, operational, and technical controls.

We concluded that the controls for the RRPS provide reasonable assurance of adequate security. Additionally, in August 2005, the FDIC started the certification and accreditation process for the RRPS, which includes extensive testing of the key controls.

Although key application controls generally operated as intended, we identified several deficiencies that posed risks to the confidentiality, integrity, and availability of the system:

- the RRPS security plan did not fully and accurately describe the current management, operational, and technical controls;
- a software configuration management plan was not fully developed or implemented; and
- read and write access rights of RRPS users were not periodically reviewed.

We therefore made three recommendations to address these risks. FDIC management agreed with the recommendations and has taken actions to address them.

Configuration Management Controls Over Operating System Software

Configuration management is a critical control for ensuring the integrity, security, and reliability of information systems. Absent a disciplined process for managing software changes, management cannot be assured that systems will operate as intended, that software defects will be minimized, and that configuration changes will be made in an efficient and timely manner. We engaged International Business Machines (IBM) Business Consulting to conduct an audit to determine whether the FDIC had established and implemented configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices.

IBM's audit concluded that the FDIC had established and implemented a number of configuration management controls over its operating system software that were consistent with federal standards and guidelines and industry-accepted practices. Such controls included a software patch management policy, a change control board, and periodic scanning of operating system software configurations.

These actions were positive; however, control improvements were needed. Specifically, the FDIC needed to establish an organizational policy and system-specific procedures to ensure proper configuration of operating system software. The FDIC also needed to standardize and integrate the recording, tracking, and reporting of operating system software configuration changes to the extent practical.

We made five recommendations to address these matters, and management has either initiated or plans to initiate actions to address them.

Money Laundering and Terrorist Financing

The nation continues to face the global threat of terrorism. In response to this threat, the Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Public Law 107-56 (USA PATRIOT Act), which expands the Treasury Department's authority initially established under the Bank Secrecy Act of 1970 (BSA) to regulate the activities of U.S. financial institutions, particularly their relations with individuals and entities with foreign ties. Specifically, the USA PATRIOT Act expands the BSA beyond its original purpose of deterring and detecting money laundering to also address terrorist financing activities. In today's global banking environment, where funds are transferred instantly and communication systems make services available internationally, a lapse at even a small financial institution outside of a major metropolitan area can have significant implications across the nation. The reality today is that all institutions are at risk of being used to facilitate criminal activities, including terrorist financing.

Through its examiners, the FDIC seeks to ensure that institutions have a strong BSA program to address money laundering and terrorist financing concerns. While many FDIC-supervised institutions are diligent in their efforts to establish, execute, and administer effective BSA compliance programs, there have been instances where controls and efforts were lacking. When such instances are identified in the course of examinations, the FDIC may request bank management to address the deficiencies in a written response to the FDIC, outlining the corrective action proposed and establishing a timeframe for implementation, or the FDIC may pursue an enforcement action.

In addition, in September 2004, the Financial Crimes Enforcement Network (FinCEN), an arm of the U.S. Treasury Department, signed an information-sharing Memorandum of Understanding with the federal banking agencies, including the FDIC. The Memorandum of Understanding requires an increased level of BSA reporting and accountability between the federal banking agencies and FinCEN. In June 2005, the FDIC, in conjunction with the other federal banking regulators, issued revisions to its BSA examination procedures.

The continuing challenge facing the FDIC is to ensure that banks maintain effective BSA programs that will ultimately create an environment where attempts to use the American financial system for money laundering or terrorist financing will be identified and ultimately thwarted.

Planned OIG work for fiscal year 2006 includes an audit to determine whether the FDIC is effectively using FinCEN data and tools in assessing the BSA and anti-money laundering programs of FDIC-supervised financial institutions. Another audit will determine the extent to which examiners are following BSA examination procedures for foreign transactions.

Protection of Consumers' Interests

In addition to its mission of maintaining public confidence in the nation's financial system, the FDIC also serves as an advocate for consumers through its oversight of a variety of statutory and regulatory requirements aimed at protecting consumers from unfair and unscrupulous banking practices. The FDIC is legislatively mandated to enforce various statutes and regulations regarding consumer protection and civil rights with respect to state-chartered, non-member banks and to encourage community investment initiatives by these institutions.

The FDIC accomplishes its mission of protecting consumers under various laws and regulations by conducting compliance

examinations and Community Reinvestment Act (CRA) evaluations. The FDIC takes enforcement actions to address compliance violations, encourages public involvement in the community reinvestment process, assists financial institutions with fair lending and consumer compliance through education and guidance, and provides assistance to various parties within and outside of the FDIC. The Corporation has also developed a program to examine institution compliance with privacy laws.

The Corporation has emphasized financial literacy, aimed specifically at low- and moderate-income people who may not have had banking relationships, and the Corporation's "Money Smart" initiative is a key outreach effort in that regard. In a related vein, protecting consumers from unscrupulous banking practices also continues to be a challenging aspect of consumer protection.

Finally, and importantly, the number of reported instances of identity theft has greatly increased in recent years, and the consequences to consumers can be devastating. The Corporation will need to remain vigilant in conducting comprehensive, risk-based compliance examinations that ensure the protection of consumer interests, analyzing and responding appropriately to consumer complaints, and educating individuals on money management topics, including identity protection and how to avoid becoming victims of various consumer scams. A challenge facing the FDIC and other regulators is protecting consumer interests while minimizing regulatory burden. The FDIC, Federal Reserve Board, and Office of the Comptroller of the Currency jointly approved amendments to CRA regulations, effective September 1, 2005, that preserve the importance of community Development in the CRA evaluations of the banks.

DSC's Risk-Focused Compliance Examination Process

In June 2003, the FDIC's DSC revised its program for examining institutional compliance with consumer protection laws and regulations. Under the new program, 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 approach to examinations. We conducted an audit to determine whether DSC's risk-focused compliance examination program results in examinations that are adequately planned and effective in assessing financial institution compliance with consumer protection laws and regulations.

We found that DSC examiners generally complied with the policies and procedures related to risk-scoping compliance examinations and that the Risk Profile and Scoping Memorandums prepared by examiners provided an adequate basis for planned examination coverage. The examiners reviewed bank policies, procedures, disclosures, and forms for compliance with consumer protection laws and regulations for each examination we reviewed and planned for transaction testing or spot checks in all compliance areas over the course of two consecutive examinations – a period of 2 to 6 years, depending on an institution's size and ratings. Additionally, examiners conducted transaction testing or spot checks in those areas for which violations had been found at previous compliance examinations.

However, we found that examination documentation did not always show the transaction testing or spot checks conducted during the on-site portion of the examinations, including testing to ensure the reliability of the institutions' compliance review functions. Examiners also did not always document whether the examination reviewed all the compliance areas in the planned scope of review. As a result, DSC cannot assure that the extent of testing was appropriate except for those areas in which

examiners had identified violations and included them in Reports of Examination.

We recommended that DSC clarify and reinforce requirements that examiners adequately document the scope of the work performed, including transaction testing and spot checks of the reliability of the institutions' compliance review functions, during the on-site portions of compliance examinations. FDIC management agreed with the recommendation and has taken corrective action.

Ongoing work in the consumer protection area includes an audit of the FDIC's efforts to address predatory lending. Two other audits are assessing (1) bank service providers' protection of sensitive customer information and (2) DSC's institution and examination guidance for implementing data privacy and security provisions of Title V of the Gramm-Leach-Bliley Act and the Fair and Accurate Credit Transaction Act. (See also the Investigations section of this report regarding the Office of Investigations' consumer protection-related work.)

Corporate Governance in the FDIC

Corporate governance within the FDIC is the responsibility of the Board of Directors, officers, and operating managers in fulfilling the Corporation's broad mission functions. It also provides the structure for setting goals and objectives, the means to attaining those goals and objectives, and ways of monitoring performance. Management of the FDIC's corporate resources is essential for efficiently achieving the FDIC's program goals and objectives.

Also, the Administration has outlined management initiatives for departments and major agencies in the President's Management Agenda (PMA). These initiatives are (1) strategic management of human capital, (2) competitive sourcing, (3) improved financial management, (4) expanded electronic government, and (5) budget and performance integration.

Although the FDIC is not subject to the PMA, it has given priority attention to continuing efforts to improve operational efficiency and effectiveness, consistent with the PMA.

We discuss corporate governance challenges at the FDIC under seven different categories below.

Management of Human Capital

Since 2002, the FDIC has been working to create a flexible permanent workforce that is poised to respond to sudden changes in the financial sector. FDIC executives announced workforce planning initiatives providing for human resources flexibilities, established a Corporate Employee Program, implemented a Buyout Program, and reorganized major corporate divisions and functions. The FDIC's training and development function, known as the FDIC Corporate University (CU), is a key ingredient in the implementation of the FDIC's Corporate Employee Program and other corporate efforts to address skill and competency requirements.

The FDIC's Corporate University

In 2003, the FDIC established the CU as a separate FDIC office to serve as the corporate umbrella over Training and Development (T&D), with responsibility for overseeing, coordinating, and supporting the assessment, design, development, delivery, and evaluation of division and office T&D programs.

We conducted an evaluation to assess (1) the degree to which CU has implemented training programs and other developmental opportunities to help the FDIC build the competencies needed to achieve its mission and strategic goals and (2) the overall cost-effectiveness of the CU structure in comparison to initial goals and industry benchmarks.

We evaluated CU's implementation of training programs and developmental opportunities using the Government Accountability Office Guide for Assessing Strategic Training and Development Efforts

in the Federal Government, which presents core characteristics for successful T&D programs. Overall, we concluded that CU has addressed, to varying degrees, each of the following Government Accountability Office core characteristics:

- Strategic alignment
- Leadership commitment and communication
- Stakeholder involvement
- Accountability and recognition
- Effective resource allocation
- Partnerships and learning from others
- Data quality assurance
- Continuous performance improvement

With regard to cost-effectiveness of the CU structure, the FDIC's 2005 budgeted T&D costs were lower than 2002 budgeted training costs. Further, we determined that CU training costs, based on a percentage of payroll, were in line with industry benchmarks. CU's ratio of training staff to employees was within the range of other selected banking regulators. Moreover, the FDIC's ratio does not consider training that CU provides to non-FDIC employees.

Competitive Sourcing

The FDIC awarded long-term contracts to consolidate outsourced information technology activities. The contract combined approximately 40 contracts into 1 contract with multiple vendors for a total program value of \$555 million over 10 years. The Corporation may face challenges in getting work completed and overseeing the large task orders.

In an audit planned for fiscal year 2006, we will address whether the task orders are being awarded consistent with sound procurement practices.

Improved Financial Management

The FDIC fielded a new financial management system during 2005 designed to consolidate the operations of multiple systems. Named the New Financial Environment (NFE), this initiative seeks to modernize the FDIC's financial reporting capabilities. Implementing NFE and interfacing other systems with NFE has required significant corporate efforts and resources.

Two audits during the reporting period addressed NFE issues, as discussed below.

NFE Testing

We engaged KPMG LLP to perform an audit of NFE testing. The audit concluded that the FDIC had developed a rigorous multi-stage test strategy and schedule for the NFE to ensure it would function as designed and meet users' needs. However, KPMG found that improvements were needed in various testing phases of NFE. As a result, financial management system integrity and financial reporting risks may not have been mitigated to an acceptable level at the time KPMG completed its audit work. We provided details of these findings as they were identified to the Division of Finance (DOF) and NFE project management team to facilitate timely corrective action and response where appropriate. We recommended that DOF and the NFE project management team review the risks identified and develop a risk resolution and action approach in accordance with the risk mitigation procedures outlined in the NFE risk management plan. Management's response to our audit addressed our concerns.

NFE System and Data Conversion

As referenced in our previous semiannual report, KPMG also began an audit seeking to review NFE system and data conversion activities. The audit objective was to determine whether systems and data conversion plans and activities were adequate to minimize the risk of errors and omissions during NFE implementation. FDIC management informed us that providing the OIG access to information would "definitely impact"

the NFE implementation schedule given the timing of planned audit tests and procedures relative to its implementation. As a result, we terminated the audit on April 6, 2005, to avoid delaying NFE implementation. We issued a report during the current reporting period summarizing KPMG's findings up to audit termination.

KPMG disclaimed from providing assurance with respect to the audit objective. KPMG was unable to collect sufficient, competent, and relevant evidence in a timely manner as required by generally accepted government auditing standards to provide a reasonable basis for audit conclusions related to the audit objective.

KPMG expressed reservations about the lack of detailed data conversion, validation, and clean-up plans for the asset management, general ledger, vendor, purchase order, accounts receivable, and cash management functions. Lack of detailed plans for these functions could have increased the likelihood of errors and omissions during the conversion process. KPMG also noted the lack of a detailed performance test plan and omitted tests that could have impacted or interrupted NFE operations. The report contained no recommendations, and a response was not required.

The FDIC's DOF responded that the conversion activity planning and execution, coupled with the active involvement of data owners from the impacted business areas in planning, testing, and validation, provided a high degree of confidence that the conversion of data would result in minimal and manageable operational disruption and conversion errors. Regarding performance testing, management indicated that "tuning" of a few functions has continued following NFE implementation. This process was expected to continue for several months, but no interruptions or delays in service were anticipated.

The FDIC's Investment Policies

The Secretary of the Treasury requires the FDIC to invest its non-appropriated cash held in the BIF and SAIF (hereafter, the

Funds) through the Government Account Series Program. The FDIC seeks to maximize investment returns, subject to overriding liquidity considerations. The FDIC considers liquidity requirements and current and prospective market conditions, including U.S. Treasury security yields, when developing quarterly investment strategies.

We engaged the firm of Pricewaterhouse Coopers, LLP (PwC) to determine whether the FDIC's investment strategy and portfolio management procedures provide the highest possible investment returns for the FDIC, taking into consideration the applicable legal and regulatory framework established for investments of the Funds.

PwC's audit concluded that the FDIC's DOF generally performed well in managing the FDIC's investment portfolio in the context of the applicable legal and regulatory framework, stated investment strategy, interest rate environment, and assessment of certain insured institutions undergoing financial stress. PwC also found no instances of non-compliance with applicable laws and regulations.

PwC identified opportunities for the FDIC to improve the return on its investments through two broad courses of action:

- In certain market environments, the FDIC should decrease holdings in overnight certificates and increase holdings in longer-maturity securities. Such holdings reduce the volatility of returns, but fail to enhance liquidity, because the Government Account Series Program investments enjoy virtually perfect transactional liquidity.
- Explore the possibility of changes in the FDIC's investment approach, such as expanding the universe of allowable investments.

The report recommended that the Corporation consider the following actions:

- Performing an internal review of investment policies to determine, among other

things, whether a limit on overnight certificates should be established.

- Using the portfolio market value for reserve ratio calculations.
- Adopting measurement techniques to compare plans with actual results.

PwC also recommended:

- Establishing goals based on volatility as opposed to liquidity.
- Retaining outside expertise to conduct periodic reviews.

When we issued our final report, three of our five recommendations were unresolved. As of the date of issuance of this semiannual report, in conjunction with FDIC program officials, the FDIC Audit Committee, and the FDIC Chairman, we have resolved all matters. With respect to establishing a dollar limit on overnight investment holdings in the BIF and SAIF in excess of the limit requiring approval, management did not agree that the additional control was needed. The OIG continues to believe that this control has value; however, management has given the recommendation sufficient consideration and provided adequate support for its position. Regarding the retention of outside experts to conduct reviews, the FDIC's management decision was that such a review would be appropriate, and management has requested the OIG to conduct an independent audit of the corporate investment program every 3 years, including policies applicable to the National Liquidation Fund. A final unresolved recommendation concerned adopting measurement techniques to compare plans with actual results. At a meeting with FDIC program representatives subsequent to issuance of our final report, we received additional information concerning fund performance management and reporting. This information, together with the audit results that the FDIC generally performed well in managing the investment

portfolio, supports the FDIC's position that sufficient action is taken to measure investment returns.

E-Government

The FDIC's E-Government Strategy is a component of the enterprise architecture that focuses on service delivery for the external customers of the FDIC. The FDIC has initiated a number of projects that will enable the Corporation to improve internal operations, communications, and service to members of the public, businesses, and other government offices. The projects include: Call Report Modernization, Virtual Supervisory Information on the Net, Asset Servicing Technology Enhancement Project, NFE, Corporate Human Resources Information System, and FDICconnect. The risks of not implementing e-government principles are that the FDIC will not efficiently communicate and serve its internal and external customers.

Implementation of E-Government Principles

We conducted an audit related to the FDIC's E-Government activities. We limited our work to obtaining an understanding of the FDIC's progress on E-Government initiatives because the FDIC had not yet developed a comprehensive E-Government strategic plan.

We determined that the FDIC has made progress in implementing various initiatives that are consistent with E-Government principles and implementing guidance from OMB. In addition, the Corporation has taken steps to develop a comprehensive E-Government strategic plan that will be linked to associated corporate goals and objectives in areas addressed by OMB's Scorecard and the E-Government Act guidance. The Corporation had established a milestone of December 31, 2005 for the approval of a new E-Government strategic plan. It actually adopted a plan in September 2005.

Although we did not make recommendations, our report suggested that in completing the new E-Government strategic plan, the Corporation be mindful of OMB's guidance that E-Government performance measures must be linked to the Corporation's Annual Performance Plan and Strategic Plan and desired outcomes of E-Government initiatives must be identified.

Risk Management and Assessment of Corporate Performance

Within the business community, there is a heightened awareness of the need for a robust risk management program. Because of past corporate governance breakdowns at some major corporations, organizations are seeking a "portfolio" view of risks and the launch of proactive measures against threats that could disrupt the achievement of strategic goals and objectives. To address these needs, a best practice has developed—enterprise risk management. Enterprise risk management is a process designed to: identify potential events that may affect the entity, manage identified risks, and provide reasonable assurance regarding how identified risks will affect the achievement of entity objectives. The Office of Enterprise Risk Management (OERM) is responsible for developing an enterprise risk management program for the FDIC. The migration from internal control to enterprise risk management perspectives and activities presents challenges and opportunities for the FDIC.

In the spirit of the Government Performance and Results Act of 1993, the FDIC prepares a strategic plan that outlines its mission, vision, and strategic goals and objectives within the context of its three major business lines; an annual performance plan that translates the vision and goals of the strategic plan into measurable annual goals, targets, and indicators; and an annual performance report that compares actual results against planned goals. In addition, the FDIC Chairman develops a supplemental set of "stretch" annual corporate performance objectives based on three strategic areas of focus that

cut across the Corporation's three business lines: Sound Policy, Stability, and Stewardship.

The Corporation is continually focused on establishing and meeting annual performance goals that are outcome-oriented, linking performance goals and budgetary resources, implementing processes to verify and validate reported performance data, and addressing cross-cutting issues and programs that affect other federal financial institution regulatory agencies.

OIG efforts addressing risk management and corporate performance assessment during the reporting period included the following.

Corporate Planning Follow-Up

In response to a request by the Corporation's Chief Financial Officer, we performed a follow-up evaluation of a July 2001 study of the Corporate Planning Cycle (CPC) that we had conducted jointly with the FDIC Office of Internal Control Management, now OERM. The objectives of the most recent review were to: determine whether DOF has been successful in reducing resources dedicated to the CPC and streamlining the CPC process; assess the FDIC's success in integrating budget and performance goal information; and benchmark the Corporation's CPC process against other agreed-upon agencies' or organizations' processes.

We concluded that DOF has made progress in reducing resources dedicated to the CPC and streamlining the CPC process. Most division and office representatives indicated that the resources and time required for the 2005 budget formulation process had been reduced. DOF streamlined the cycle time for the budget formulation exercise from over 6 months for the 2001 budget to 3 months for the 2005 budget. Nevertheless, division and office representatives expressed concerns regarding several areas in the budget process, and we concluded that DOF could make several improvements to the FDIC's planning and budget process.

The FDIC has also made progress in integrating budget and performance goal infor-

mation. For the 2005 corporate operating budget, the FDIC used an approach that involved senior management decisions on strategic and annual initiatives at the onset of the budget formulation exercise; provided budget representatives planning and budget formulation guidelines developed through senior management discussion; and required divisions and offices to review and provide input for performance plans, performance objectives, and proposed baseline operating budgets. This approach was an improvement over the 2001 CPC process wherein the staffing, budgeting, and planning processes overlapped and were not as well integrated.

Our report contained three recommendations to help ensure that divisions and offices have adequate information to review and respond to (1) proposed budgets in the areas of information technology services and external training and (2) requests for proposed increases or decreases to their respective budgets. Another recommendation was intended to help the FDIC communicate and institutionalize the streamlined planning and budget process.

DOF generally concurred with our four recommendations, and we consider management's actions taken or planned responsive. We benchmarked the FDIC's CPC process against other selected federal agencies' planning and budget processes and provided this information for management's use.

Management of Major Projects

Project management involves defining, planning, scheduling, and controlling the tasks that must be completed to reach a goal and allocating resources to perform those tasks. The FDIC has engaged in several multi-million dollar projects, such as the NFE project discussed earlier, Central Data Repository, and Virginia Square Phase II Construction. Without effective project management, the FDIC runs the risk that corporate requirements and user needs may not be met in a timely, cost-effective manner.

In September 2002, the FDIC established the Capital Investment Review Committee (CIRC) as the control framework for determining whether a proposed investment is appropriate for the FDIC Board of Directors' consideration, overseeing approved investments throughout their life cycle, and providing quarterly capital investment reports to the Board. The CIRC generally monitors projects valued at more than \$3 million. The FDIC later developed the Chief Information Officer's Council to recommend and oversee technology strategies, priorities, and progress. The work of the Council encompasses the entire portfolio of technology projects, including those below the threshold addressed by the CIRC.

Beginning with the 2003 budget, the FDIC began budgeting and tracking capital investment expenses as a separate component of the budget to enhance management's ability to focus on such projects. Project funds established within the investment budget are to be available for the life of the project rather than for the fiscal year. Final responsibility for approving the initial creation or modification of a project's capital investment budget rests with the FDIC's Board of Directors. In addition, the Division of Information Technology has recently adopted the Rational Unified Process system development life cycle model and has established a Program Management Office. Both of these initiatives should result in additional oversight and control mechanisms for corporate projects.

Virginia Square Phase II Construction

As the Corporation's Virginia Square Phase II construction project progressed, we conducted an evaluation to determine whether: (1) project costs were within budget and tasks were being completed on schedule, (2) the FDIC was following its established project control framework, and (3) the Division of Administration (DOA) had planned for space utilization in light of corporate downsizing.

We concluded that the Virginia Square Phase II project costs are within budget and that tasks are being completed on schedule. Also,

the FDIC is effectively following its established project control framework. Further, DOA is planning for space utilization in light of corporate downsizing and has analyzed several options for disposition of vacant space at Virginia Square. We validated most of the assumptions used in those options. The report contains no recommendations. However, we encouraged DOA to work with the Division of Information Technology to develop more precise estimates of anticipated on-site contractor staffing at Virginia Square because the cost-benefit of one of the options was, in part, dependent on a sufficient number of contractors performing work at Virginia Square.

CDR Project Management

Financial institutions regulated by the Call Report agencies are required to submit quarterly Consolidated Reports of Condition and Income, commonly referred to as Call Reports. To improve the regulatory call reporting process, the FDIC, on behalf of the Call Report agencies, entered into a \$39 million contract with Unisys Corporation for the central data repository (CDR) system. The contract consists of a phased approach for implementing the new call reporting process. Among other benefits, the CDR system (1) would provide data to the industry more quickly in a manner that allows more flexibility for data analysis and (2) would increase efficiencies, resulting in a cost savings of \$27 million over the 10-year life of the contract. The contract was modified in January 2005 to address industry feedback and allow more time for system testing and enrollment. The modification revised the system deployment date from October 2004 to September 2005. The CDR Steering Committee was established to oversee the system development effort under this contract and includes representatives from the Federal Reserve Board, the Office of the Comptroller of the Currency, and the FDIC.

During the reporting period we conducted an audit to determine whether CDR project management was adequate. We concluded that the CDR project management team had established adequate project management controls. However, the CDR project has

been faced with both management and technical challenges associated with fielding new technology across multiple platforms, highly diverse users, and adopting new business practices associated with the call reporting process. The project team has been unable to overcome the challenges, and implementation of the CDR system was delayed for at least 1 year. This lack of progress raised concerns as to whether system functionality as originally envisioned could be attained. The report contains three recommendations intended to address the additional risks associated with the delayed implementation of system functionalities. The Corporation's response to the draft report addressed the concerns we identified and was responsive to our recommendations.

Cost Containment and Procurement Integrity

As steward for the BIF, SAIF, and the Federal Savings and Loan Insurance Corporation Resolution Fund, the FDIC strives to identify and implement measures to contain and reduce costs, either through more careful spending or by assessing and making changes in business processes to increase efficiency. A key challenge to containing costs relates to the contracting area. To assist the Corporation in accomplishing its mission, contractors provide a variety of services. To contain costs, the FDIC must ensure that its acquisition framework—its policies, procedures, and internal controls—is marked by sound planning; consistent use of competition; fairness; well-structured contracts designed to result in cost-effective, quality performance from contractors; and vigilant oversight management to ensure the receipt of goods and services at fair and reasonable prices.

Several of our assignments during the reporting period addressed cost containment and procurement issues. We evaluated two aspects of FDIC employee travel and also looked at the Corporation's contract solicitation and evaluation process, as discussed below.

FDIC Management of Travel Costs

The FDIC contracted with the Scheduled Airlines Traffic Offices, Inc. (SatoTravel) to perform travel reservation services for FDIC employees. SatoTravel assists the FDIC's travelers in making official travel arrangements that are consistent with the FDIC's travel policies, cost considerations, and employee preferences, in that order. The FDIC executed the SatoTravel contract in August 2002 with 1 base year and four 1-year options. The total compensation ceiling for the 5-year contract period is \$900,000. One of our evaluations during the reporting period was designed to determine whether the FDIC and SatoTravel are efficiently and effectively managing travel costs and requirements under the contract.

We determined that the FDIC can improve monitoring and controls over its travel program. Specifically, DOF suspended a requirement for bank examiners to make lodging reservations through SatoTravel, which, in turn, reduced the amount of rebates the FDIC received under the contract for hotel reservations. As a result, DOF is exceeding the SatoTravel contract compensation ceiling amount. We estimated that the FDIC may exceed the 5-year contract compensation ceiling price by \$367,000—a contract increase of 40 percent. In late July 2005, DOA approved additional funding to cover anticipated contract costs through September 2006.

In addition, the FDIC could further reduce travel costs and increase program controls by increasing the number of travelers that stay in hotels that offer commissions to the FDIC and use SatoTravel's on-line reservation system to make lodging arrangements. Further, DOF requires the use of the government-issued travel card only for airfare costs. Requiring the use of the government travel card for all travel costs, including airline, hotel, and car rental would achieve modest savings in the form of rebates from the travel card sponsor bank, strengthen management control over the travel program by providing better information for planning and negotiating travel services, and promote internal consistency.

Finally, most government agencies are required to use the General Services Administration's (GSA) eTravel Program by 2006. The goal of the eTravel program is to centralize the federal government's travel process and reduce administrative travel expenses. Although the FDIC is not required to use the eTravel program, it could improve or eventually replace the FDIC's current travel program.

We made five recommendations to bring about improvements to the program. Management agreed with four of our five recommendations and considered but elected not to reinstate the policy requiring mandatory use of the national travel agency for bank examiners.

Inside Board Member and Executive Manager Travel

The FDIC General Travel Regulations (GTR) governs employee travel. The FDIC expects all employees traveling on official business to exercise the same prudent care in incurring reimbursable expenses as though traveling on personal business. The FDIC's DOF is responsible for maintaining the GTR, processing travel expense reimbursement vouchers and, when appropriate, auditing travel claims. The FDIC's Board of Directors and Executive Managers (EM) have heightened visibility as corporate leaders and frequently travel to represent the FDIC. (For the purpose of our report, we referred to both Executive Managers and inside Board members as EMs.)

We performed an evaluation to determine whether EM travel was authorized, approved, and paid in accordance with the GTR. Our review focused on temporary duty travel from July 1, 2002 through September 30, 2004 for 3 inside Board members and 89 EMs. We selected a judgmental sample of 25 vouchers based on traveler frequency and expense claim amounts.

We found that EM travel for the vouchers reviewed was not always authorized in accordance with the GTR, and travel claims that were paid were not always allowable. Fur-

ther, neither supervisory reviews nor DOF audits of EM vouchers routinely detected unauthorized or unallowable claims. These control deficiencies over the administration of the FDIC's travel program created an environment in which travel was not always authorized and expenses were not always claimed and paid according to the GTR.

We made recommendations related to reemphasizing certain travel policies to EMs, revising travel audit procedures, and ensuring that risk-based travel audits are effectively implemented.

Management agreed with four of our five recommendations and proposed an alternative action that sufficiently addresses the fifth recommendation. Management's responsive actions were promptly communicated to all corporate EMs.

Contract Solicitation and Evaluation Process

We conducted an audit to determine if the FDIC (1) achieved adequate price competition in its contract solicitation process in order to obtain fair and reasonable prices for goods and services and (2) complied with the Acquisition Policy Manual (APM) solicitation and proposal evaluation requirements.

We determined that the Acquisition Services Branch generally complied with the APM's solicitation and evaluation requirements. Further, the Acquisition Services Branch achieved adequate price competition for the purpose of obtaining fair and reasonable prices. However, the FDIC did not always request price reductions on contracts awarded through GSA's Multiple Award Schedule (MAS) program. Requesting price reductions from MAS contractors could result in more favorable pricing due to market fluctuations that cause discounts to be offered.

We recommended that DOA revise the APM to require the contracting officer to seek price reductions on contracts awarded through GSA's MAS program unless there are extenuating circumstances, or based on price analysis or other assessment, the con-

tracting officer determines that the MAS contract price represents the best value at the lowest possible price. In such cases, the contracting officer should be required to document the reason for not seeking a price reduction.

DOA did not agree that the APM should be modified. However, DOA agreed that the contracting officer must adequately document the basis for determining that prices are fair and reasonable and represent the best value for the FDIC. DOA has reminded the contracting officers of their responsibility to evaluate and document price evaluations and has established a training program related to price evaluation. DOA's alternative corrective actions were responsive.

Other work related to this challenge during the reporting period included two post-award contract billing audits. The billing reviews identified \$981,355 in questioned costs. Management is currently addressing the findings in those audits.

Resolution and Receivership Activities

One of the FDIC's key responsibilities is planning and efficiently handling the franchise marketing of failing FDIC-insured institutions and providing prompt, responsive, and efficient resolution of failed financial institutions. There has been a significant decline in bank failures over the past several years. However, planning models for responding to failing and failed institutions, including large or multiple bank failures, need to be evaluated, revisited, and tested for adequacy in light of the impact of recent corporate and external events. These include FDIC downsizing activities, the continued threat of terrorist-related activities, and natural disasters that change the operating environment in which FDIC resources must react.

In addition, the Division of Resolutions and Receiverships (DRR) faces other challenges

from an information system enhancement project, the Asset Servicing Technology Enhancement Project (ASTEP), which is intended to create an integrated solution to meet the FDIC's current and future asset servicing responsibilities based on industry standards, best practices, and adaptable technology. Successfully implementing ASTEP is an important aspect of DRR mission achievement.

DRR's Pre-closing Planning Process

During the reporting period, we audited DRR's pre-closing planning process for resolving troubled and failed FDIC-insured financial depository institutions.

Based on our survey work, we found that DRR had a structured and efficient bank resolution process and concluded that, overall, DRR's pre-closing planning process was adequate. Accordingly, we decided to conclude our field work after completion of the audit survey, and we made no recommendations in this report. We did, however, suggest that in light of DRR downsizing, DRR may need to reconsider the existing internal control structure for the pre-closing planning process given the substantive changes in its operations.

We also had an ongoing audit of DRR's ASTEP program during the reporting period, the objective of which was to determine project management effectiveness in developing and deploying the ASTEP solution.



Investigations: Making an Impact

The Office of Investigations (OI) carries out the investigative mission of the OIG. Agents in Washington, D.C.; Atlanta; Dallas; and Chicago conduct investigations of alleged criminal or otherwise prohibited activities that may harm or threaten to harm the operations or integrity of the FDIC and its programs. OI also operates an Electronic Crimes Unit (ECU) and laboratory in Washington, D.C. The ECU is responsible for conducting computer-related investigations impacting the FDIC, including employee cases involving computer abuse, and providing computer forensic support to investigations nationwide. OI also manages the OIG Hotline for employees, contractors, and others to report allegations of fraud, waste, abuse, and mismanagement via a toll-free number or e-mail.

We concentrate our investigative efforts on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Another consideration in dedicating resources to these cases is the need to pursue appropriate criminal penalties not only to punish the offender but to deter others from participating in similar crimes.

Currently, 73 percent of our caseload is comprised of investigations involving financial institution fraud. The focus of our work in this area is on

- FDIC-supervised institutions
- Fraud by officers, directors, or insiders
- Obstruction of examinations

Investigative Statistics April 1, 2005—September 30, 2005

Judicial Actions:

Indictments/Informations	22
Convictions	19

OIG Investigations Resulted in:

Fines of	\$13,000
Restitution of	\$4,932,490
Other Monetary Recoveries of	\$463,895
Total	\$5,409,385

Cases Referred to the Department of Justice (U.S. Attorney)

29

Referrals to FDIC Management

1

OIG Cases Conducted Jointly with Other Agencies

80

- Fraud leading to the failure of the institution
- Fraud impacting multiple institutions
- Fraud involving monetary losses that could significantly impact the institution

As referenced earlier in this report, many of these cases address instances of failed corporate governance. That is, in a number of situations, the senior executives of the financial institution are involved in unscrupulous activities that cause serious problems and even failures of the institutions.

In addition to pursuing financial institution-related cases, the OIG commits resources to investigations that target fraud by FDIC debtors seeking to conceal their assets from the FDIC. These cases made up 15 percent of our caseload as of September 30, 2005.

The FDIC was owed more than \$1.7 billion in criminal restitution as of September 30, 2005. In most instances, the individuals subject to these restitution orders do not have the means to pay. The focus of OIG investigations in this area is on those individuals who do have the means to pay, but hide their assets and/or lie about their ability to

pay. OI works closely with the Division of Resolutions and Receiverships (DRR) and the Legal Division in aggressively pursuing investigations of these individuals.

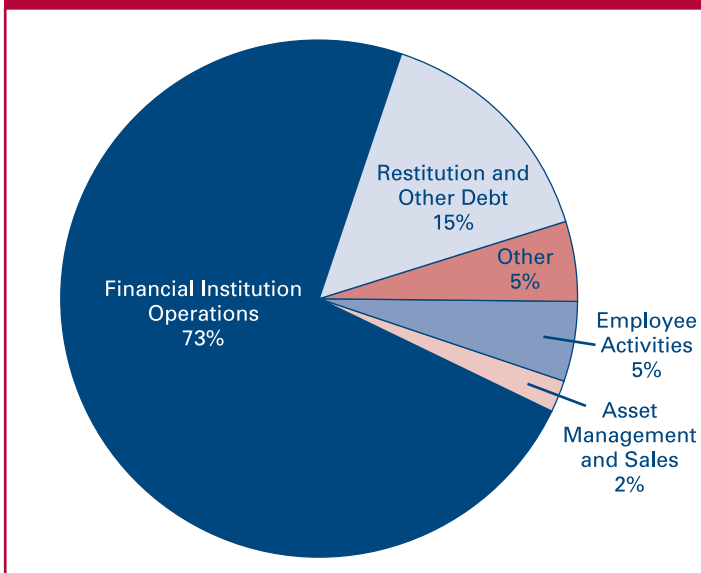
Although currently only about 5 percent of our caseload, the OIG must commit resources to investigations of criminal or serious misconduct on the part of FDIC employees. These are among the most sensitive of OIG cases and are critical to ensure the integrity of, and public confidence in, FDIC operations. Other cases may address consumer protection matters, such as misrepresentations regarding FDIC affiliation or insurance. Several such cases are described later in this section.

Joint Efforts

The OIG works closely with U.S. Attorneys' Offices throughout the country in attempting to bring to justice individuals who have defrauded the FDIC. The prosecutorial skills and outstanding direction provided by Assistant U.S. Attorneys with whom we work are critical to our success. The results we are reporting for the last 6 months reflect the efforts in the U.S. Attorneys' Offices in the Central District of Illinois, District of Colorado, District of Nebraska, District of Connecticut, District of Minnesota, District of South Carolina, Northern District of Texas, Northern District of Iowa, District of New Mexico, Northern District of Mississippi, Western District of Oklahoma, District of Alaska, and the Eastern District of Virginia. In addition to working with local U.S. Attorneys' Offices, the OIG worked with trial Attorneys from the Fraud Section of the U.S. Department of Justice and State Prosecutors from the Missouri Attorney General's Office.

Support and cooperation among other law enforcement agencies is also a key ingredient for success in the investigative community. We frequently "partner" with the Federal Bureau of Investigation (FBI), the Internal Revenue Service Criminal Investigation Division (IRS CID), the U.S. Postal Inspection Service, and other law enforcement agencies

Figure 2: Office of Investigations Case Distribution (as of September 30, 2005)



in conducting investigations of joint interest.

Also vital to our success is our partnership with FDIC program offices. We coordinate closely with the FDIC's Division of Supervision and Consumer Protection (DSC) in investigating fraud at financial institutions, and with DRR and the Legal Division in investigations involving failed institutions and fraud by FDIC debtors. Our ECU coordinates closely with the Division of Information Technology in carrying out its mission. The successes highlighted for the period would not have been possible without the collaboration of these offices.

In addition to carrying out its direct investigative responsibilities, the OIG is committed to providing training and sharing information with FDIC components and other regulators based on "lessons learned" regarding red flags and fraud schemes identified through our investigations. OI agents provide training and frequently give presentations to FDIC staff during regional and field office meetings. We are also called upon by the Federal Financial Institutions Examination Council, state banking regulatory agencies, and law enforcement agencies to present case studies.

"The type of scheme alleged in today's indictment brings to mind the familiar saying, 'If it looks too good to be true, it probably is.'"

**U.S. Attorney
Jan Paul Miller**
commenting on
indictment of
land "flipping" scheme

Results

Over the last 6 months, OI opened 33 new cases and closed 18 cases, leaving 130 cases underway at the end of the period. Our work during the period led to indictments or criminal charges against 22 individuals and convictions of 19 defendants. Criminal charges remained pending against 34 individuals as of the end of the reporting period. Fines, restitutions, and recoveries resulting from our cases totaled \$5,409,385.

The following are highlights of some of the results from our investigative activity over the last 6 months.

Fraud Arising at or Impacting Financial Institutions

Three Businessmen Charged in \$8 Million Real Estate "Land Flip" Scheme

A federal grand jury in the Central District of Illinois returned an 11-count superseding indictment adding a third businessman to a rental real estate land flipping scheme in Decatur, Illinois. The 11-count superseding indictment charged the three businessmen with bank fraud, mail fraud, money laundering, and wire fraud.



Property purchased at fraudulently inflated prices.

From 1999 through 2005, the defendants allegedly engaged in a real estate land flipping scheme to defraud real estate lenders, including Central Illinois Bank, Champaign, Illinois, an FDIC-insured institution, buyers and sellers. The scheme involved more than 150 fraudulent real estate sales and financing transactions totaling more than \$8 million in fraud against financial institutions.

The superseding indictment alleged that the defendants used fraudulent appraisals to buy, sell, and finance properties at prices fraudulently inflated. Two of the defendants falsely represented themselves as property managers who were in the business of buying, selling, and managing real estate. The third defendant was a licensed real estate appraiser who allegedly performed numerous appraisals for the two defendants in which he falsely inflated the value of the real estate.

To carry out the scheme, two of the defendants recruited buyers, typically of modest means with little or no experience in rental real estate investment. To entice the buyers, the two defendants allegedly made one or more representations to them regarding prospective properties:

- they would be paid as much as \$5,000 for each property purchased;
- they could purchase properties for no money down;
- the properties were worth the appraised amounts;
- assistance would be provided in making loan applications to mortgage lenders;
- the two defendants would act as the buyer's property manager, and would locate tenants and collect the rents;

- the two defendants would make the loan payments directly to the mortgage lenders; and
- the two defendants would buy back the properties on a contract for deed.

The two businessmen allegedly made more than \$3 million for their personal use and to promote the scheme, while the real estate appraiser received fees of \$350 to \$450 per appraisal.

Joint investigation by the FDIC OIG, the U.S. Postal Inspection Service and the FBI; prosecuted by the U.S. Attorney's Office for the Central District of Illinois.

Jury Finds Two Defendants Guilty in Connection with BestBank Failure

After a 3-week trial in the U.S. District Court in Denver, 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, Boulder, Colorado.

By way of background, the defendants operated a portfolio of subprime credit cards issued by BestBank from 1994 through 1998. When BestBank was closed in July 1998, its largest asset was the portfolio of subprime credit card accounts with a reported value of more than \$200 million. 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.

From 1994 through July 1998, the defendants engaged in a

“This type of scheme diminishes confidence in our national banking system; the defendants in this case personally made a tremendous amount of money at the expense of Americans who rely on our banking system.”

U.S. Attorney Bill Leone commenting on guilty verdicts in BestBank investigation



Travel club marketing materials

business operation that made more than 500,000 BestBank credit card loans to subprime borrowers. In July 1998, 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, with losses exceeding \$200 million.

BestBank entered into agreements with Century Financial and the defendants to market 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 subprime 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 even their membership materials.

The jury found that the defendants carried out a fraudulent scheme in several ways.

Most people did not pay the mandatory \$20 fee required before the account was funded. Over 50 percent of the subprime borrowers' accounts were non-performing. The defendants and Century Financial fraudulently concealed the subprime borrowers' non-performance and delinquency rates by reporting non-performing accounts as performing. The defendants paid \$20 to some accounts so they would appear to be performing when in fact they were not.

Also charged in the BestBank failure are the former owner, chief executive officer and chairman of the board of directors; the former president and director; and the former chief financial officer and director. The case against these three defendants is pending and no trial date has been set.

The defendants each received more than \$5 million during the course of the fraudulent scheme. Each of them faces a possible mandatory minimum sentence of 10 years to life in federal prison and fines of up to twice the amount gained from committing the offense.

Joint investigation by the FDIC OIG, the FBI, and the IRS CID; prosecuted by the U.S. Attorney's Office for the District of Colorado and the U.S. Department of Justice.

Former Vice President of Bank of Sierra Blanca Arrested on Bank Fraud Charges

A federal grand jury in the U.S. District Court for the Western District of Texas returned a 21-count indictment against the former vice president of Bank of Sierra Blanca (BSB), Sierra Blanca, Texas. The grand jury charged the defendant with 1 count of bank fraud and 20 counts of misapplication of bank funds.

By way of background, on January 18, 2002, the Bank of Sierra Blanca was closed, and the receiving bank, Security State Bank of Pecos was renamed TransPecos Sierra Blanca Bank. The indictment alleges that from about 1995 until November 2001, the defendant devised a scheme to fraudulently obtain money, funds, credits, assets, securities, and other

property owned by and under the control of the Bank of Sierra Blanca. The defendant allegedly abused her position of trust within the bank, lied to bank personnel and customers, made false entries in bank records, and stole bank money and credit. The defendant allegedly misapplied money from the accounts of the bank by various means, including over drafting checking accounts, obtaining funds through unauthorized transfers, using bank and customers' funds to pay personal debts and debts of others, and causing the bank to pay unauthorized interest rates on deposits. The indictment further alleged that the defendant attempted to conceal her activities by making false entries in the bank's accounting system, creating a fictitious account under her control, and misapplying additional money and credit from other accounts of the bank and using those funds to replenish accounts victimized by previous thefts.

Through her scheme, the defendant allegedly converted approximately \$1.2 million belonging to the bank and its customers for her personal use.

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

Former President of Deuel County State Bank Sentenced to 4 Years in Prison

The former president of the Deuel County State Bank (DCSB), Chappell, Nebraska, was sentenced in the U.S. District Court for the District of Nebraska. Earlier, the defendant pleaded guilty to a one-count bill of information charging him with bank fraud. He received 4 years' imprisonment, 5 years' supervised probation upon release, and was ordered to pay \$1.9 million in restitution.

This case was initiated based on information reported by DSC and DRR indicating that DCSB, an institution supervised by the Federal Reserve was near failure as a result of a check kiting and fraudulent loan scheme perpetrated by the defendant. The kiting was conducted between DCSB and a sister institution, Haxtun Community Bank, Haxtun,

Colorado, an FDIC-insured institution. The losses from the scheme were approximately \$1.8 million. The defendant admitted that between August 27, 2001, and July 30, 2003, he defrauded DCSB by making approximately \$745,000 in loans to himself without board approval. This amount exceeded the bank's limits of money that can be loaned to bank insiders. As part of the defendant's plea agreement, he stipulated to an action under Section 8(e) of the Federal Deposit Insurance Act, which provides a lifetime ban from banking.

Joint investigation by the FDIC OIG, FBI, and Federal Reserve Board OIG; prosecuted by the U.S. Attorney's Office for the District of Nebraska.

Former Bank President of Connecticut Bank of Commerce Pleads Guilty

The former president of Connecticut Bank of Commerce, Stamford, Connecticut, pleaded guilty in the U.S. District Court for the District of Connecticut to a one-count criminal information charging him with misapplication of bank funds.

According to the information, the defendant, at the direction of the former chairman of the Connecticut Bank of Commerce board of directors, caused a \$1.35 million loan to be made to an entity known as Moore Advisors, Inc. (Moore), and further caused the loan proceeds to be wired to a bank account held in the company's name. At the time the loan was made, the defendant knew that no Board approval had been obtained for the loan, which was required; knew he had no documentation to suggest that Moore had any assets, income, or other means to support the loan; and knew that the natural effect of his actions was to put the bank at substantial risk of loss.

The former chairman of the Connecticut Bank of Commerce board of directors was sentenced in January 2005 to 51 months' incarceration and 36 months' supervised release after pleading guilty to one count of misapplication of bank funds. No criminal restitution was ordered by the court because

the parties agreed that the former chairman's payment of \$8.5 million to the FDIC as part of his settlement of the agency's administrative charges satisfied all losses directly related to his criminal conduct.

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

Former Bank President at Town & Country Bank Sentenced and Former State of Minnesota Representative Found Guilty in Bank Failure

The former president of Town & Country Bank of Almelund (T&C Bank), Almelund, Minnesota, was sentenced in the District of Minnesota to 18 months' incarceration with 3 years' supervised release and was ordered to pay \$1.35 million in restitution to the FDIC.

The defendant earlier pleaded guilty to 1 count of conspiracy to commit bank fraud and 1 count of money laundering of an 11-count superseding indictment charging him with bank fraud, money laundering, false bank entries, and conspiracy. The superseding indictment alleged that the defendant and others executed a scheme to defraud the former T&C Bank by manipulating over 20 false lines of credit that resulted in the failure of the bank in July 2000 when the State of Minnesota declared the bank insolvent and appointed the FDIC as receiver. The failure of T&C Bank resulted in an estimated loss of \$3.4 million to the FDIC Bank Insurance Fund.

Former State of Minnesota Representative Found Guilty

After a 2-week trial in July 2005 in the District of Minnesota, a former State of Minnesota Representative was found guilty on two counts of mail fraud and one count of money laundering in connection with his activity with the former T&C Bank. He was found not guilty on two other counts of mail fraud, one other count of money laundering, and one count of conspiracy.

During the Representative's tenure in the Minnesota House, he served as the chairman

of the House Regulated Industries Committee, which oversaw the legislation regarding utility companies. According to the indictment, the Representative used his position to enact legislation permitting utility companies to use energy conservation funds for research and development projects. Once the legislation was enacted, he used his position to coerce the utility companies to pay \$650,000 in grants to Northern Pole, a Minnesota corporation created to recycle old utility poles. The Representative had a significant equity stake in Northern Pole.

The Representative had a personal and business relationship with the former president of T&C Bank. As alleged in the indictment, the two devised a scheme whereby the defendant would invest in Northern Pole, a troubled credit of T&C Bank. The scheme involved borrowing money from T&C Bank in the name of the Representative's other businesses, diverting those funds to Northern Pole and other troubled credits of the bank, and using State of Minnesota grant money to pay back the debt service on the loans.

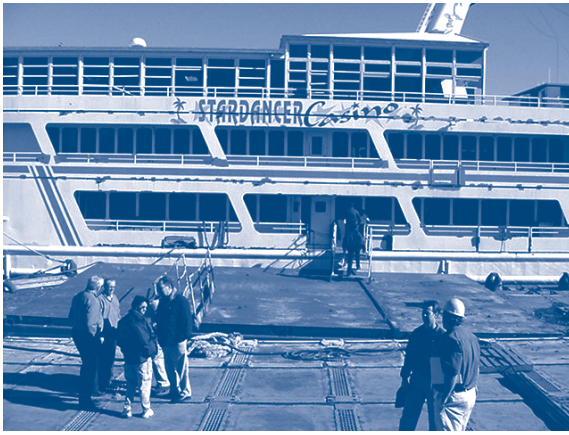
Throughout this investigation, OIG agents have been coordinating with DSC, DRR, and the Legal Division.

Joint investigation by the FDIC OIG, the FBI, and the IRS CID; prosecuted by the U.S. Attorney's Office for the District of Minnesota.

Owners of Stardancer Casinos, Inc. Indicted on Tax Fraud

In the District of South Carolina, Florence Division, the owners of Stardancer Casinos, Inc., (Stardancer) of Duluth, Georgia, were charged in an 18-count indictment with tax fraud for the period April 2001 to November 2002.

The president and chief executive officer of Stardancer and the executive vice president operated casino boats in Little River, South Carolina, and several locations in Florida from February 1999 through January 2003. The defendants were charged with withholding employment taxes from Stardancer employees' payroll checks and failing to pay



One of Stardancer's gambling vessels seized by the government.

those taxes to the U.S. government, resulting in a loss to the government of approximately \$1.15 million.

The investigation into Stardancer was initiated in February 2002, when the former president of the Oakwood Deposit Bank Company, Oakwood, Ohio, confessed to embezzling over \$40 million from Oakwood Deposit Bank Company, which led to the bank's insolvency. The former president admitted that most of the money was embezzled to Stardancer. Investigators eventually determined that over \$43 million was embezzled to Stardancer and ultimately shut down the company in January 2003, with the execution of search warrants and seizure of Stardancer's gambling vessels and shuttle craft. The former president pleaded guilty to embezzlement and money laundering and was sentenced to 14 years' imprisonment and was ordered to pay \$48,718,405 in restitution.

Joint investigation by the FDIC OIG, the IRS CID, and FBI; prosecuted by the U.S. Attorney's Office for the District of South Carolina.

Additional Indictments

Four Business Associates Charged in \$2.16 Million Real Estate Fraud Scheme

A federal grand jury in the Northern District of Texas returned a seven-count indictment

against three business associates employed by BetterHomes of Dallas and an employee of American Title and Capital Title of Dallas. The seven-count indictment charged the four defendants with bank fraud, mail fraud, wire fraud, and conspiracy.

The indictment alleged that from December 2002 through March 2004, the four defendants engaged in a real estate scheme to defraud various real estate lenders, buyers, and sellers, including Fremont Investment and Loan, an FDIC-supervised institution. The indictment alleged that the three defendants from BetterHomes of Dallas recruited straw purchasers and borrowers to purchase and finance single-family residences they had located and submitted fraudulent loan documents to the lenders in the name of the straw borrowers indicating the down payment for the loans had been made by the borrowers. The employee of the title company would release the loan proceeds early to the three defendants from BetterHomes, who would then purchase cashiers' checks in the name of the straw borrowers to obtain loans in an amount greater than the value of the residences. The indictment further alleged that 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. The three defendants also executed contracts between their company, BetterHomes of Dallas, and the straw borrowers stating the company would be responsible for the loans, but they 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.

Former Vice President of Republic Bank Indicted on Bank Fraud

The Grand Jury in the U.S. District Court for Minnesota indicted the former vice president and loan officer of Republic Bank, Duluth, Minnesota, on one count of bank fraud.

This case was initiated based on a referral from DSC, Kansas City, following the defen-

dant's removal from Republic Bank. The indictment alleged that the defendant made a series of fraudulent loans that benefited him personally and caused a loss to Republic Bank of approximately \$608,000. The defendant allegedly embezzled the funds by using a variety of fictitious loans, nominee loans, and fraudulent loans to family members. He also allegedly forged a number of bank officers' signatures on documents and created false documents to support loan fund disbursements. He is also charged with converting two repossessed automobiles to his own use.

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

Former Executive Vice President of Iowa-Nebraska State Bank Indicted

The former executive vice president of Iowa-Nebraska State Bank, South Sioux City, Nebraska, converted \$125,000 in an unsecured loan to a bank customer and falsely stated that the purpose of the loan was for "operating expenses" and "for the purchase (down payment) of video lottery machines" when in fact the defendant knew that the borrower was going to transfer the loan proceeds back to him. The defendant used the proceeds of the loan for his personal benefit, including paying off his two daughters' car loans. The defendant was indicted in the U.S. District Court for the Northern District of Iowa on two counts of making false entries in bank records.

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

Guilty Pleas

Former Officer of New Mexico Bank Pleads Guilty to Bank Fraud

A former assistant vice president of Citizens Bank, Farmington, New Mexico, pleaded guilty in the District of New Mexico to a one-count information charging her with bank fraud. The defendant admitted to submitting fraudulent debit and credit tick-

ets, which caused funds to be credited to an inactive customer bank account. After the inactive account was credited with the funds, the defendant transferred the funds to her personal bank accounts. She continued her scheme by requesting cash from bank tellers and then submitting fraudulent debit and credit tickets to cover up and balance the transactions. Losses attributed to this scheme resulted in approximately \$667,658 being fraudulently obtained from Citizens Bank.

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

Former President of Garnavillo Savings Bank Pleads Guilty to Bank Fraud

The former president of Garnavillo Savings Bank, Garnavillo, Texas, pleaded guilty in the U.S. District Court for the Northern District of Iowa to a one-count information charging him with bank fraud. He admitted to executing a scheme between 1996 and 2003 to embezzle funds of more than \$157,000 from Garnavillo Savings Bank. As part of his plea agreement, the former president stipulated to an action under Section 8(e) of the Federal Deposit Insurance Act, which provides a lifetime ban from banking, and he also agreed to pay \$157,009 in restitution.

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

Bank Customer Pleads Guilty to Bank Fraud

A bank customer from Omaha, Nebraska, pleaded guilty to one count of bank fraud in the U.S. District Court of Nebraska. In February 2004 the defendant was indicted on charges from a check-kiting scheme he engaged in during 2000. The indictment alleged that the defendant kited checks between accounts maintained at Nebraska State Bank and Mid-City Bank for his personal and business purposes. Losses from the check-kite totaled approximately \$2.7 million.

DSC provided the information leading to the joint investigation by the FDIC OIG and FBI; prosecuted by the U.S. Attorney's Office for the District of Nebraska.

Bank Borrower Pleads Guilty to Bank Fraud

A borrower at the State Bank of Belle Plaine, Belle Plaine, Minnesota, pleaded guilty in the U.S. District Court for the District of Minnesota to a one-count information charging her with bank fraud. The defendant participated in the accounts receivable purchase loan program with the State Bank of Belle Plaine and admitted to creating and submitting fraudulent invoices causing the bank to advance approximately \$107,000 on false invoices.

Joint investigation by the FDIC OIG, FBI, and U.S. Secret Service; prosecuted by the U.S. Attorney's Office for the District of Minnesota.

Sentencings

Bank Customer Sentenced in Bank of Falkner's Failure

In the continuing investigation of the September 2000 failure of the Bank of Falkner, Falkner, Mississippi, a bank customer was sentenced in the Northern District of Mississippi to serve 36 months in prison followed by 60 months of supervised release. He was also ordered to pay restitution to the FDIC in the amount of \$1.16 million. The bank customer's sentence resulted from an earlier guilty plea to a two-count criminal information charging him with making and causing false entries in the books, reports, and statements of the Bank of Falkner, with respect to a series of nominee loans he received. He was also charged with money laundering in connection with his use of the proceeds of the nominee loans.

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

Former Executive Vice President of Minnwest Bank South Sentenced

The former executive vice president and chief loan officer for Minnwest Bank South, Slayton, Minnesota, converted bank funds to his financially troubled business, initiated nominee loans, and made false entries to conceal the true status of the nominee loans from the FDIC and other bank officers. The former executive vice president pleaded guilty to conspiracy to commit bank fraud in the District of Minnesota and was sentenced to 5 months' imprisonment, and 3 years' supervised release. He was ordered to pay \$37,000 in restitution to Minnwest Bank South, and he stipulated to an action under Section 8(e) of the Federal Deposit Insurance Act, which provides a lifetime ban from banking.

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

Former Cashier Sentenced for Bank Embezzlement

A former cashier of First State Bank, Canute, Oklahoma, was sentenced in the U.S. District Court for the Western District of Oklahoma. The defendant, who had earlier pleaded guilty to a one-count information charging her with bank embezzlement, received 12 months and 1 day of incarceration, 3 years of supervised release, and was ordered to pay \$122,547 in restitution. The investigation revealed that the defendant misappropriated and embezzled \$122,547 in cash from customer accounts by altering approximately 63 customer deposits. The defendant altered bank records in an effort to conceal her activities and disguise the paper trail associated with the transactions. As part of the defendant's plea agreement, she stipulated to an action under Section 8(e) of the Federal Deposit Insurance Act, which provides a lifetime ban from banking.

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

Former Employees of Stevens Financial Group Sentenced in Sinclair National Bank Failure

In past semiannual reports, we have reported a number of results of investigations and prosecutions involving the failure of Sinclair National Bank, which caused a loss of \$4.5 million to the Bank Insurance Fund. During the reporting period, an attorney and a public accountant and former operations manager for the now defunct Stevens Financial Group (SFG) and a contractor to Sinclair National Bank were sentenced in St. Louis County Circuit Court in Missouri, regarding the securities fraud investigation. The attorney pleaded guilty to one count of false statements and was sentenced to 2 years' probation and ordered to surrender his law license. The accountant and former operations manager pleaded guilty to two counts of false statements and was sentenced to 5 years' probation, and ordered to pay \$25,000 in restitution to the State of Missouri and to perform 1,000 hours of community service.

The defendants admitted that they and others created false and misleading documents to inflate the net worth of SFG by over \$10 million. The investigation disclosed that the defendants created millions of dollars in fraudulent notes receivable to assist SFG officials in disguising SFG's negative net worth. SFG sold over \$15 million in subprime loans to Sinclair National Bank, an institution that failed in September 2001. Sinclair National Bank incurred substantial losses on these subprime loans and the losses ultimately caused the failure of the bank.

Joint investigation by the FDIC OIG, FBI, and Treasury OIG; prosecuted by the Missouri Attorney General's Office and the Fraud Section of the U.S. Department of Justice, Washington, D.C.

Restitution and Other Debt Owed to the FDIC

FDIC Debtor Sentenced to 28 Months in Prison for Making False Statement

An FDIC debtor from Del Ray Beach, Florida, was sentenced in the U. S. District Court, District of Connecticut, to 28 months in prison to be followed by 3 years' supervised release; 300 hours of community service; and was ordered to continue making payments of his remaining \$2.7 million restitution debt owed to the FDIC as a result of his 1996 bank fraud conviction.

The debtor had earlier pleaded guilty to making a false statement. He and his girlfriend were previously indicted after our investigation developed evidence that they had participated in a scheme to fraudulently conceal assets from the FDIC. During the plea hearing, the defendant admitted that he had made a false statement concerning his ownership of a \$100,000 U.S. Treasury Bond. He also acknowledged that in a response to an interrogatory sent to him by the U.S. Attorney's Office, he represented that he did not possess or have any interest in any bonds when, in truth, he maintained an account with a brokerage firm in which the bond, with a cash value of approximately \$70,000 was held. The defendant also made significant income through his various business endeavors such as a used-car business, yacht brokerage activities, and real estate transactions, all of which he failed to disclose to the U.S. Probation Office.

The defendant's girlfriend pleaded guilty to assisting him in his concealment of assets from the FDIC and was earlier sentenced to 6 months' incarceration and 3 years' probation; she was also ordered to pay a fine of \$5,000 and to perform 150 hours of community service. She admitted that she knew the defendant owed \$2.7 million in restitution and that she assisted him in later concealing his assets by permitting him to buy and sell real estate in her name.

This case was investigated by the FDIC OIG; prosecuted by the U.S. Attorney's Office, District of Connecticut.

FDIC Debtor Makes Full Payment of Restitution

While under investigation by the OIG for allegedly concealing assets from the FDIC, an FDIC debtor paid in full his outstanding restitution obligation of \$453,894 to the FDIC. The defendant had been subject to the restitution order since his 2003 guilty plea for defrauding Alaska State Bank.

The defendant had previously claimed he had no access to money and was not able to make restitution payments. Based on information received from an anonymous source, the OIG learned that the residence of the defendant's daughter had been paid off. This information was provided to the U.S. Attorney's Office for the District of Alaska. When the defendant's daughter was notified that her financial records had been subpoenaed, a check for full restitution was remitted to the FDIC by the defendant's wife.

The OIG coordinated with the Legal Division and the District of Alaska Financial Litigation Unit to assist the U.S. Attorney's Office in making this collection.

Misrepresentation Regarding FDIC Affiliation

Brokers Plead Guilty to Mail Fraud

Two brokers pleaded guilty in the U.S. District Court for the Northern District of Texas to Count 57 of an 88-count superseding indictment, which charged both defendants with mail fraud. The defendants were co-owners of San Clemente Securities, Inc., (SCS) and United Custodial Corporation (UCC), located in San Clemente, California.

Beginning in early June 1995 and continuing through April 2001, SCS advertised FDIC-insured certificates of deposit at interest rates greater than those available from financial

institutions. The investors' certificates of deposit were custodialized and held in the name of UCC. The defendants falsely and fraudulently failed to advise investors nationwide that SCS and UCC would subtract undisclosed fees ranging from 3 percent to 57 percent of the amount invested. They made false representations regarding FDIC insurance coverage of the certificates of deposit. The investment confirmations and statements they sent to investors were false and intentionally misleading, and money paid to investors when they liquidated an investment prior to maturity was actually money invested by another investment or by other persons. The investors had no ownership in any investment that would be purchased in UCC's name. In 1997, SCS, along with its co-owners, had been banned by the National Credit Union Administration from doing business with federally insured credit unions because of their deceptive practices. Sentencing for both defendants is scheduled for December 2005.

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

Identity Theft

Former National Institutes of Health Federal Credit Union Employee Pleads Guilty to Bank Fraud and Identity Theft

A former National Institutes of Health Federal Credit Union (NIH FCU) administrative assistant pleaded guilty to a two-count information charging her with conspiracy to commit bank fraud and identity theft in the U.S. District Court in the Eastern District of Virginia.

Investigation determined that in March 2004, the defendant defrauded the NIH FCU by using the identities of FDIC employees to open accounts and apply for loans at the NIH FCU. The defendant was provided the identifiers of approximately 27 current and former FDIC employees by a co-conspirator. The defendant then opened accounts in each

employee's name. Once the accounts were opened, the co-conspirator applied on-line for loans and when the loans were approved, the funds were deposited electronically into each account. The defendant would then prepare and submit withdrawal slips for funds from these accounts. The defendant concealed the fraudulent scheme by making minimal monthly payments on each of the loans with funds obtained from other fraudulent loans.

Due to the defendant's knowledge of the internal controls and her position within the NIH FCU, she was able to maintain this scheme for nearly 12 months before the fraud was discovered. The defendant fraudulently obtained nearly \$450,000 in loans, and the NIH FCU recognized a loss of nearly \$435,000. The defendant's co-conspirator has not yet been charged.

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

Electronic Crimes Unit Activities

The OIG ECU continued its support of ongoing FDIC OIG investigations by providing computer forensic assistance. Specifically, the ECU imaged and analyzed 25 new computer hard drives during the reporting period. In addition, the ECU conducted keyword searches on new and existing electronic evidence producing thousands of search hits that were potentially helpful in ongoing OIG cases. The ECU also found relevant documents and e-mails in support of OIG cases.

The ECU also assisted the FDIC's Division of Information Technology in investigating employee misuse of FDIC computer resources. The ECU assisted the Division of Information Technology in two cases during the reporting period by determining whether any criminal activity occurred in relation to the misuse of FDIC computers. Specifically, the ECU analyzed computer hard drives of FDIC employees accused of accessing porno-

graphic materials to determine whether any child pornography existed on the hard drives. None of the hard drives analyzed contained any known child pornographic images.

Based on discussions with the FDIC's Division of Information Technology, the ECU also investigated six instances of alleged fictitious banks on the Internet that falsely advertised FDIC insurance. As a result, all six of the bank Web sites were deactivated.

Two Individuals Sentenced in Relation to FDIC Phishing Case

As previously reported, the ECU has been investigating a phishing scam involving the fraudulent use of the FDIC Web page. The scheme involved the use of a spam e-mail threatening cancellation of FDIC account insurance and a link to a fictitious Web site that was made to look like the FDIC Web page. The fictitious Web site asked for customer account and credit card information that would be used as part of an identity theft scheme. The subjects were previously arrested and convicted as part of the identity theft ring associated with the phishing scheme. One of the defendants was sentenced to 6 years in prison, and the other defendant was sentenced to 4 years in prison by the Leeds Crown Court, Leeds, England. The OIG continues to work on this case with the FBI, the U.S. Secret Service, and the National High-Tech Crimes Unit from the United Kingdom.

Other Highlights

Electronic Crimes Unit Presentation to DSC Information Technology Examiners

OIG's ECU gave a presentation to a group of DSC Information Technology Examiners from the Technology Supervision Branch. The presentation included a PowerPoint presentation that covered the formation and responsibilities of the ECU as well as an overview of computer forensics. The ECU also provided the group with a tour of the ECU forensic lab that included a demonstration of the forensic equipment and software

used by the ECU. Additionally, the ECU discussed and demonstrated the variety of computer equipment and media on which the ECU can perform forensic analysis. The ECU answered questions from the DSC examiners, and both sides agreed that our groups can profit greatly by working together and sharing information in the future.

FDIC OIG Honors Federal Prosecutor

Special Agent in Charge Tom McDade and Special Agent Cindy Van Noy presented Assistant United States Attorney, Arnie Huftalen, District of New Hampshire, Concord, New Hampshire, with a plaque for his successful prosecution of an FDIC debtor who provided false financial information in an affidavit of his financial condition to the FDIC. Also in connection with this case, the OIG acknowledged Robert Schwarzlose, DRR, Dallas, whose efforts contributed to the successful prosecution of the debtor.



L to R: Arnie Huftalen, Cindy Van Noy, and Tom McDade.

OIG Special Agent Honored at U.S. Attorney's Office Awards Ceremony

On June 14, 2005, the United States Attorney's Office, District of Connecticut, held its 2005 United States Attorney's Awards Ceremony at the Aldermanic Chambers, New Haven, Connecticut. The purpose of the ceremony was to acknowledge a select number of significant prosecutions adjudicated during the past year and honor those who had contributed to the success of these prosecutions. Special Agent Gary Sherrill from the OIG OI was among the honorees at the ceremony. Special Agent Sherrill was

commended for his exceptional work in a joint investigation with the FBI and IRS CID in the prosecution of the former Chairman of the Board of Directors of Connecticut Bank of Commerce.



L to R: Assistant U.S. Attorney Christopher (Kit) Schmeisser; Special Agent Gary Sherrill; Special Agent Jeffrey Bonwell, FBI; and Special Agent Thomas Buchanan, FBI.

FDIC OIG Recognizes State Prosecutors

Special Agent in Charge Tom McDade and Special Agent C. Edward Slagle presented Liz Bock, Assistant Attorney General, and Ron Carrier, Chief Counsel, Missouri Attorney General's Office, with a plaque recognizing them for their outstanding work during the prosecution of Sinclair National Bank.



L to R: Ed Slagle, Tom McDade, Ron Carrier, and Liz Bock.

OIG Employees Receive Letter of Commendation from the FBI

On August 26, 2005, Special Agent C. Ed Slagle and Laura Zach, OIG Auditor, received a letter of commendation from the FBI Kansas City Office. The commendation recognized Special Agent Slagle and Ms. Zach for their outstanding efforts during the investigation of the Sinclair National Bank case.



L to R: Tom McDade, Laura Zach, Ed Slagle, and Acting Assistant Inspector General Sara Gibson.

OI Assistance at the Center for Missing and Exploited Children

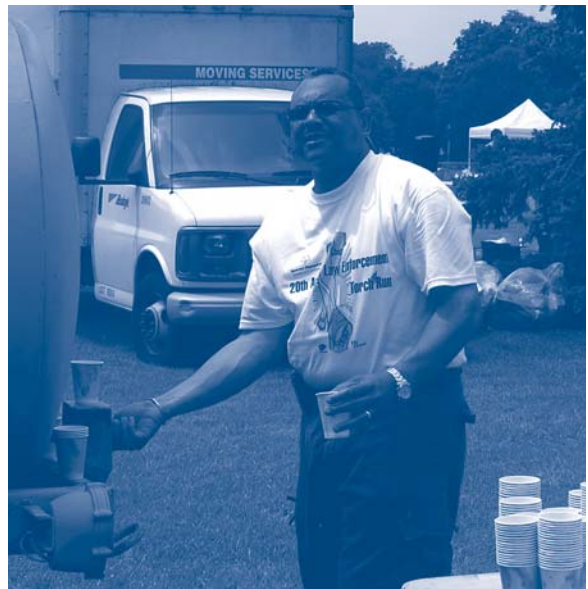
OI provided the Center for Missing and Exploited Children with law enforcement personnel to provide assistance in responding to the overwhelming volume of calls the Center was receiving by individuals trying to locate their families as a result of Hurricane Katrina.



Pictured (top to bottom) Special Agents Karen Davis and Valerie Vines Toyer. Not pictured – Joan Dwyer and Matt Alessandrino.

OIG Special Agents Participate in 20th Annual Law Enforcement Torch Run

OI staff participated in the 20th Annual Law Enforcement Torch Run/Walk to benefit the D.C. Special Olympics. The Law Enforcement Torch Run for Special Olympics D.C. is organized and conducted by over 40 federal and local law enforcement agencies. This annual project helps unify the law enforcement community, while enhancing the lives of over 2,000 local children and adults with developmental disabilities. Funds generated from the project underwrite the cost of the annual Special Olympics Summer Games.



OIG Office of Investigations' staff assisting in the Torch Run.



OIG Organization: Pursuing OIG Goals

Our office continued to aggressively pursue our four main OIG goals and related objectives during the reporting period. These goals and objectives form the blueprint for our work. While the audit, evaluation, and investigative work described in the earlier sections of this report drives our organization and contributes very fundamentally to the accomplishment of our goals, a number of other activities and initiatives complement and support these efforts and enhance the achievement of our goals. Some examples follow.

Value and Impact

OIG products will add value by achieving significant impact related to addressing issues of importance to the Chairman, the Congress, and the public. This goal means that we contribute to ensuring the protection of insured depositors, safety and soundness of FDIC-supervised institutions, protection of consumer rights, achievement of recovery to creditors of receiverships, and effective management of agency resources. Efforts in support of this goal and related objectives include the following:

- Issued 23 audit and evaluation reports containing \$981,355 in potential monetary benefits and 39 nonmonetary recom-

mendations. As discussed earlier in this report, these reports address the management and performance challenges facing the Corporation, as we identified them in December 2004.

- Conducted investigations that resulted in 22 indictments/informations; 19 convictions; and approximately \$5.4 million in total fines, restitution, and other monetary recoveries.
- Performed 16 policy analyses on proposed FDIC directives or proposed revisions to directives. We raised policy suggestions regarding the draft directives, specifically in the areas of the Risk-Related Premium System and information technology (IT) security risk management. We also offered other suggestions to strengthen or clarify the draft policies.
- Continued coordination of our Electronic Crimes Unit with Division of Supervision and Consumer Protection (DSC), Legal Division, and Division of Information Technology officials to establish appropriate processes in addressing cyber crimes, including computer intrusion, phishing and spoofing schemes, and investigations of computer misuse by FDIC employees and contractors.

- Participated in an advisory capacity at meetings of the Audit Committee's IT Security Subcommittee and FDIC Chief Information Officer's Council.
- Responded to the Corporation's solicitation of comments for proposed changes to audit and reporting requirements for insured institutions (Notice of Proposed Rulemaking, C.F.R. Part 363, Annual Independent Audits and Reporting Requirements).
- Attended the Division of Administration's Labor and Employee Relations seminar to discuss the role of the OIG's Electronic Crimes Unit in computer abuse cases.
- Commented on Division of Information Technology's E-Government Strategic Plan.
- Met, along with members of FDIC corporate management, with staff of House and Senate Banking Committees to discuss the unauthorized release of FDIC employee data.
- Formulated Fiscal Year 2006 Assignment Plan and provided draft listing of assignments to corporate management and the FDIC Vice Chairman in his role as Chairman of the Audit Committee. Briefed the Audit Committee on the proposed assignments in the plan.
- Attended meetings of the Interagency Bank Fraud Working Group.
- Participated in the FDIC's Fraud Conference. OI, along with Assistant U.S. Attorneys gave three presentations at the conference related to OI's investigative work.
- Attended DSC's New York Regional Conference, where one of our investigators gave a presentation on the Connecticut Bank of Commerce case.
- Attended meetings of the FDIC's Hurricane Task Force.
- Attended Hurricane Katrina Fraud Task Force meetings organized by the Department of Justice. The Department of Justice is relying on OIGs to play a major role in addressing fraud in Hurricane Katrina recovery efforts and has asked OIGs to publicize their efforts in this regard.
- Established a Web page, as part of the Department of Justice's Hurricane Katrina Fraud Task Force, to provide contact information to financial institutions and consumers in an effort to combat fraud in areas affected by the hurricane.
- Provided assistance to the Center for Missing and Exploited Children in efforts to help locate family members who were separated from one another as a result of Hurricane Katrina.
- Met with audit representatives of other financial regulatory OIGs (National Credit Union Administration, Department of the Treasury, Federal Reserve Board) to discuss potential audits of hurricane relief and recovery efforts.

Communication and Outreach

Communications between the OIG and the Chairman, the Congress, employees, and other stakeholders will be effective. We seek to foster effective agency relations and communications, congressional relations and communications, OIG employee relations and communications, and relations and communications with other OIG stakeholders. Efforts in support of this goal and related objectives include the following:

- Conducted seventh OIG Client Survey to solicit views of corporate management on OIG products, processes, and services.
- Participated in OIG/Legal/DRR quarterly meetings.
- Played an active role in the Federal Audit Executive Council. Our Assistant Inspectors

tor General for Audits is the Chair of the Federal Information Security Management Act (FISMA)/Information Security Committee of the Council. Our Office of Audits took the lead role in planning the annual Federal Audit Executive Council conference held in April 2005.

- Met with the Government Accountability Office staff regarding the New Financial Environment, the OIG's overall IT coverage, and FISMA work.
- Continued to attend the President's Council on Integrity and Efficiency (PCIE) Inspections and Evaluations and the Government Performance and Results Act Roundtable meetings to share information and best practices with attendees.
- Participated at the PCIE/Executive Council on Integrity and Efficiency Annual Conference at which our Assistant Inspector General for Audits gave a presentation on IT Auditing.
- Made a presentation to participants in the Corporate Employee Program to provide information on the OIG mission and work.
- Provided briefing materials to the new FDIC Vice Chairman to familiarize him with the FDIC OIG and its work at the Corporation.
- Shared results of OIG work posted on our Web site through the FDIC's Online Subscription Service.
- Met with staff from the House and Senate Appropriations Committees regarding the OIG's fiscal year 2006 appropriation request.
- Met with Office of Management and Budget, at its request, regarding proposed fiscal year 2007 budget.
- Briefed staff from the House Financial Services and Senate Banking, Housing, and Urban Affairs Committees on completed audits, evaluations, and investiga-

tions; planned reviews; and possible legislative ideas.

- Informed House and Senate oversight committee staff members of online availability of selected OIG reports as such reports were made publicly available.
- Continued ongoing meetings between the Executives of the OIG and the FDIC's Division and Office Heads in both headquarters and regional offices to foster and sustain successful cooperation and communication in all aspects of our audit, evaluation, and investigative activities. The Office of Investigations continued presentations in lessons learned/red flags based on its experience with failed institutions.
- Coordinated with Inspectors General, Assistant Inspectors General for Audits, and Assistant Inspectors General for Investigations of federal financial institution regulatory agencies.
- Provided highlights reports to the FDIC Chairman to keep him informed of significant OIG events.
- Presented the results of OIG audit and evaluation work at monthly meetings of the Audit Committee. These meetings bring senior management attention to OIG findings, recommendations, and related issues of significance.

Human Capital

The OIG will align its human resources to support the OIG mission. We aim to enhance our workforce analysis and planning, competency investments, leadership development, and the development of a results-oriented, high-performance culture. Efforts in support of this goal and related objectives include the following:

- Convened meetings of the OIG's Employee Advisory Group. This group provides feedback to the Inspector General/Deputy Inspector General on the working conditions and business

processes of the office and keeps OIG staff informed of current issues of employee concern.

- Participated in corporate diversity initiatives and programs throughout the reporting period.
- Initiated a mentoring program for employees who have recently joined the OIG and new supervisors. The program will be designed to enhance employees' job skills, empower employees, and promote good organizational citizenship.
- Participated in the Inspector General Community's pilot implementation of e-learning through SkillSoft. By leveraging technology, this program is designed to offer quality training to OIG staff in a cost-effective, efficient manner.
- Participated in the Leadership Training Program of the PCIE at the Federal Executive Institute in Charlottesville, Virginia.

Productivity

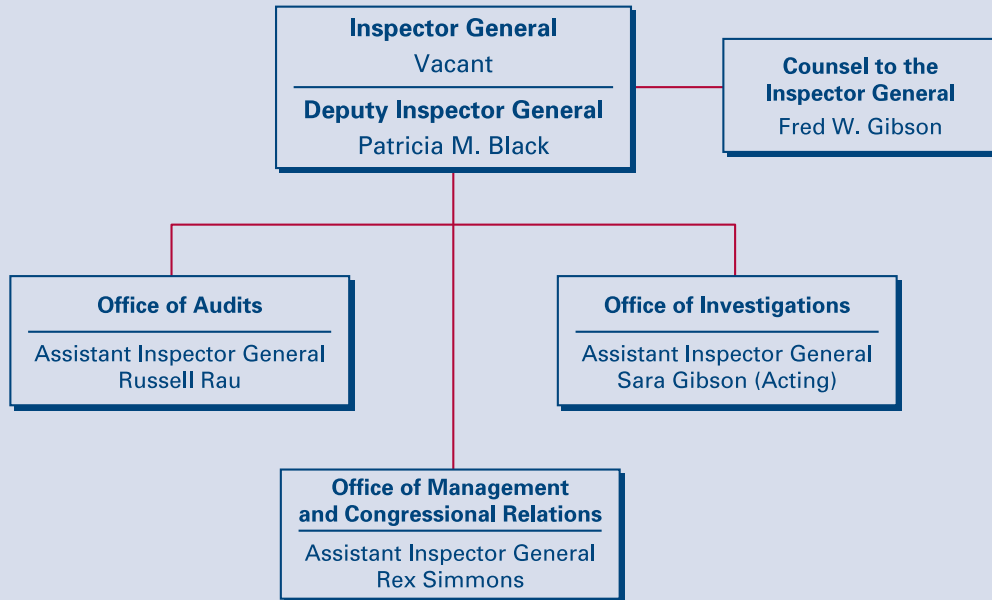
The OIG will effectively manage its resources. We have taken steps to contain OIG costs and undertook several initiatives to ensure that our processes are efficient and that our products meet quality standards. Efforts in support of this goal and related objectives include the following:

- The OIG's fiscal year 2006 budget for \$29,965,000 (\$160,000 less than the Congress appropriated for fiscal year 2005) is awaiting congressional approval. The 2006 budget represents the OIG's tenth consecutive budget decrease after adjusting for inflation.
- Announced planned closure of the OIG's audit offices in Atlanta and Chicago as part of an effort to downsize and consolidate certain Office of Audits operations.
- Issued the OIG's Fiscal Year 2005 Performance Report reporting progress on achievement of 37 annual perfor-

mance goals reflecting OIG emphasis on (1) adding value by achieving impact on issues of importance to the Corporation and our other stakeholders; (2) fostering effective communications with our stakeholders; (3) aligning human resources to support the OIG mission; and (4) managing our resources effectively. We met or substantially met 31, or 84 percent, of the 37 goals.

- Announced reorganization of Office of Audits directorates—from six to three—to complement the Corporation's principal operational areas: Insurance, Supervision, and Receivership Management Audits; Systems Management and Security Audits; and Corporate Evaluations and Audits.
- Restructured operating components by eliminating quality assurance and oversight office and transferring staff and functions of that office to Office of Management and Congressional Relations and Office of Audits.
- Installed upgraded TeamMate software to enhance auditors' maintaining of workpapers.
- Met with the Division of Information Technology on issues related to enhancing the OIG's IT security.
- Modified manner in which OIG policies are maintained and disseminated—moving from electronic and hard copy system to electronic posting of policies on our Intranet Web site, for enhanced efficiency.
- Formed working group to address enhanced methods for strategically planning and focusing OIG efforts.

OIG Organization Chart



Points of Contact

Title	Name	Telephone Number
Inspector General	Vacant	
Deputy Inspector General	Patricia M. Black	202-416-2026
Counsel to the Inspector General	Fred W. Gibson	202-416-2917
Assistant Inspector General for Audits	Russell Rau	202-416-2543
Deputy Assistant Inspector General for Audits	Stephen Beard	202-416-4217
Acting Assistant Inspector General for Investigations	Sara Gibson	202-416-2920
Assistant Inspector General for Management and Congressional Relations	Rex Simmons	202-416-2483

OIG Counsel Activities (April–September 2005)

The Office of Counsel (OC) provides independent legal advice and assistance to the Inspector General and the staff of the OIG. During the latter half of fiscal year 2005, OC engaged in wider multi-disciplinary activities, reflecting the current needs of a greater range of OIG stakeholders. OC represented the OIG at the Department of Homeland Security’s Inspector General Roundtable on security issues facing the Inspector General community. In the aftermath of Hurricane Katrina, OC participated in the Department of Justice’s Hurricane Katrina Fraud Task Force and engaged in discussions with other federal banking regulators to determine collaborative work dealing with the post-Katrina restoration efforts. Internally, OC participated in the development of a new process for enhanced planning and implementation of OIG work. Other activities from the reporting period are described below:

Litigation	OC represented the OIG in personnel cases before the Equal Employment Opportunity Commission, Merit Systems Protection Board, and in litigation before the District Courts for the District of Columbia and the Middle District of Florida. OC was involved in 28 litigation-related matters, 3 of which were resolved during the period, and the remainder of which are awaiting further action.
Advice and Counseling	OC provided advice and counsel, written opinions, and determinations of legal applicability on issues arising during the course of audits, investigations, and evaluations. Examples include analysis of: the statutory authority of the Inspector General; the applicability of privacy-related laws and regulations to the FDIC and its operations; banking law matters including the FDIC’s Maximum Efficiency, Risk-focused, Institution Targeted and compliance examination procedures, and the use of corrective and enforcement actions; the FDIC’s deposit insurance assessment program; and ethics-related and investigative matters. OC provided input in conjunction with briefings of congressional committees, and met with Congressional staff in support of Congressional oversight matters. Counsel’s Office provided comments relative to the legal accuracy and sufficiency of more than 14 audit and evaluation reports.
Legislation/Regulation Review	OC reviewed proposed legislation S. 1332, the Personal Data Privacy and Security Act of 2005, and reviewed and commented on three proposed formal FDIC regulations, seven FDIC directives, and two OIG policies.
Subpoenas	OC prepared 10 subpoenas for issuance during this reporting period.
Freedom of Information and/or Privacy Act	OC responded to four requests under the Freedom of Information Act.

**Table 1: Significant OIG Achievements
(April–September 2005)**

Audit and Evaluation Reports Issued	23
Questioned Costs	\$981,355
Investigations Opened	33
Investigations Closed	18
OIG Subpoenas Issued	10
Convictions	19
Fines, Restitution, and Monetary Recoveries	\$5.4 million
Hotline Allegations Referred	38
Proposed Regulations and Legislation Reviewed	4
Proposed FDIC Policies Reviewed	16
Responses to Requests and Appeals Under the Freedom of Information Act	4

Table 2: Nonmonetary Recommendations

April 2003–September 2003	103
October 2003–March 2004	51
April 2004–September 2004	86
October 2004–March 2005	37
April 2005–September 2005	39

Figure 3: Products Issued and Investigations Closed

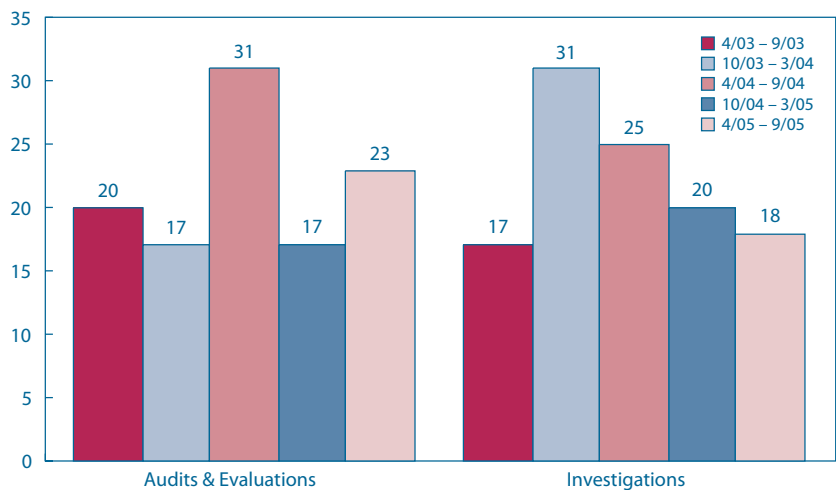


Figure 4: Questioned Costs/Funds Put to Better Use (\$ in millions)

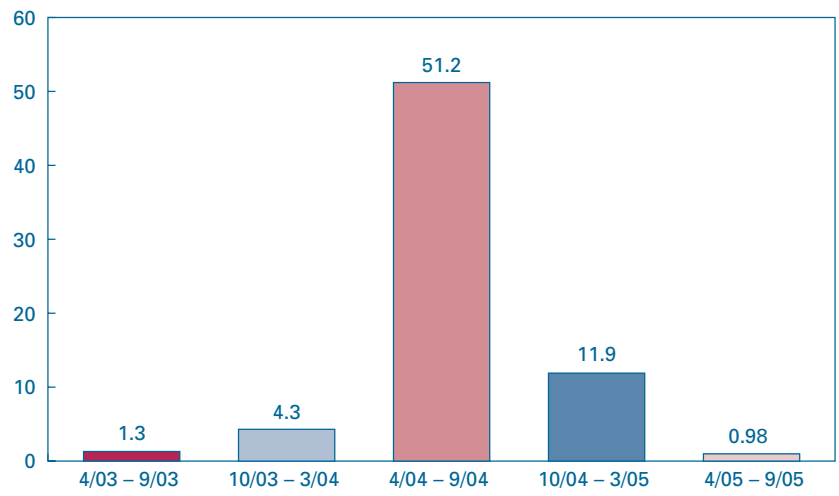
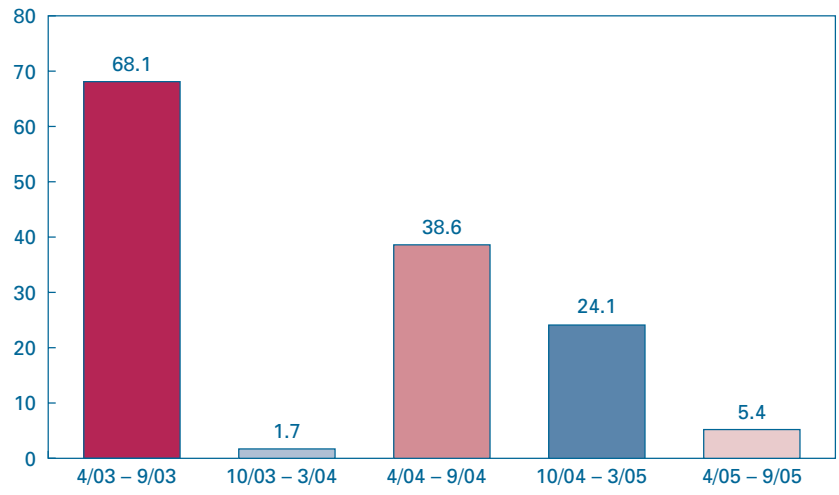


Figure 5: Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations (\$ in millions)





Fiscal Year 2005 Performance Report Summary

This Performance Report Summary presents a brief overview of our performance compared to our fiscal year (FY) 2005 annual performance goals. It provides a statistical summary as well as narrative summary of performance results by strategic goal area. The full version of our performance report is available on our Web site at www.fdicig.gov.

The four overall strategic goals, each with a number of performance goals that we have pursued during FY 2005 are shown in the following table, which provides a statistical summary of our performance against the performance goals for FY 2005. The table

reflects the number of performance goals that were **Met**, **Substantially Met**, or **Not Met**.

As shown in the table, overall we met or substantially met 31 of our 37 performance goals (84 percent) in FY 2005. For the previous reporting period (FY 2004), we had a 76-percent level of achievement of goals met or substantially met. We recognize that organizational performance should not be evaluated based solely on a statistical summary of measures – given that all measures are not equal in weight and the quality of the measures is still evolving.

A summary discussion of our performance by strategic goal is presented below.

Strategic Goals	FY 2005 Annual Performance Goal Accomplishment (Number of Goals)			
	Met	Substantially Met	Not Met	Total
OIG Products Add Value and Achieve Significant Impact	6	1	3	10
Communication with Stakeholders Is Effective	6	0	1	7
Human Resources Are Aligned to Support the OIG Mission	2	1	0	3
The OIG Effectively Manages Resources	12	3	2	17
Total	26	5	6	37
Percentage	70%	14%	16%	100%

Strategic Goal 1:

OIG Products Add Value and Achieve Significant Impact

We met or substantially met 7 of our 10 performance goals to add value and achieve significant impact with our products and services under Strategic Goal 1. Of particular note, we achieved a 1.73 to 1 ratio of monetary benefits to operating costs for our audit operations, as measured over a 3-year period. In other words, we received a return of \$1.73 for each dollar spent on our audit operations over the past 3 years. This exceeded our goal of achieving a 1:1 ratio. On the investigation side, 80 percent of our investigation cases that were accepted for prosecution resulted in convictions, pleas, and/or settlements, which exceeded our target of 70 percent.

On a less positive note, we concluded that we did not meet two goals related to improving client satisfaction with our audit, evaluation, and investigation functions. As reflected in our annual client survey, FDIC executives voiced concerns about various aspects of our core functional areas. Many of these were similar to those raised in previous client surveys. We have developed action steps to address these concerns as well as other opportunities for improvement identified through the survey. We also recognize that a certain tension between the OIG and its clients may be inherent in the nature of our mission and have some bearing on client survey results.

Strategic Goal 2:

Communication with Stakeholders Is Effective

We met or substantially met six of our seven performance goals to foster effective communications and outreach with our stake-

holders under Strategic Goal 2. Significant efforts in support of this strategic goal during the year included cosponsoring an Emerging Issues in Banking symposium with the Federal Reserve Board and Department of the Treasury OIGs, hosting an open house in our Electronic Crimes Unit laboratory for FDIC executives, and continuing to meet regularly with FDIC executives and managers in both headquarters and regional offices.

Strategic Goal 3:

Human Resources Are Aligned to Support the OIG Mission

We met or substantially met all three of our performance goals to align human resources to support the OIG mission under Strategic Goal 3. Key results under this strategic goal included establishing an OIG mentoring program and participating in the Inspector General community's pilot implementation of e-learning training courses.

Strategic Goal 4:

The OIG Effectively Manages Resources

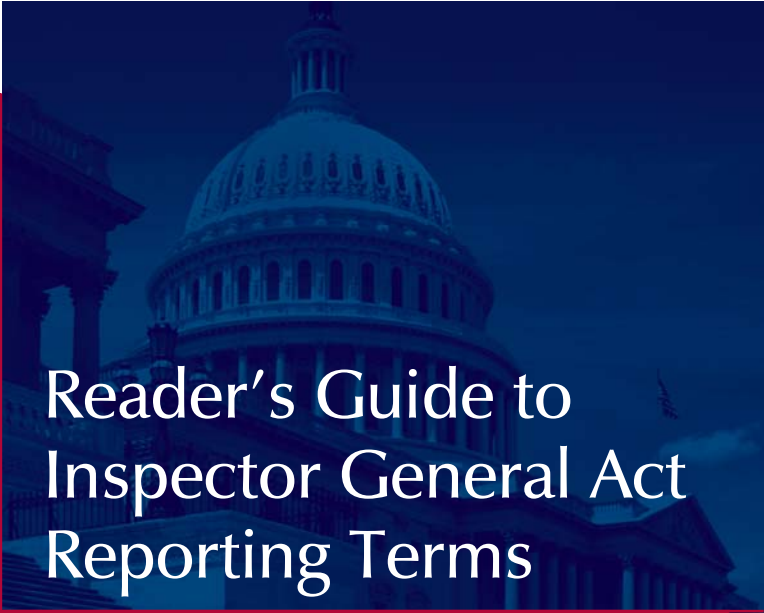
We met or substantially met 15 of our 17 performance goals to effectively manage OIG resources under Strategic Goal 4. One of our accomplishments under this strategic goal was to develop a new Web-based Investigations Data System that will significantly improve the previous system's availability and performance through improved technology.



Reporting Requirements

Index of Reporting Requirements—Inspector General Act of 1978, as amended

Reporting Requirement	Page
Section 4(a)(2): Review of legislation and regulations	46
Section 5(a)(1): Significant problems, abuses, and deficiencies	7-24
Section 5(a)(2): Recommendations with respect to significant problems, abuses, and deficiencies	7-24
Section 5(a)(3): Recommendations described in previous semiannual reports on which corrective action has not been completed	54
Section 5(a)(4): Matters referred to prosecutive authorities	25
Section 5(a)(5) and 6(b)(2): Summary of instances where requested information was refused	59
Section 5(a)(6): Listing of audit reports	57
Section 5(a)(7): Summary of particularly significant reports	7-24
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs	58
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	59
Section 5(a)(10): Audit recommendations more than 6 months old for which no management decision has been made	59
Section 5(a)(11): Significant revised management decisions during the current reporting period	59
Section 5(a)(12): Significant management decisions with which the OIG disagreed	59



Reader's Guide to Inspector General Act Reporting Terms

What Happens When Auditors Identify Monetary Benefits?

Our experience has found that the reporting terminology outlined in the Inspector General Act of 1978, as amended, often confuses people. To lessen such confusion and place these terms in proper context, we present the following discussion:

The Inspector General Act defines the terminology and establishes the reporting requirements for the identification and disposition of questioned costs in audit reports. To understand how this process works, it is helpful to know the key terms and how they relate to each other.

The first step in the process is when the audit report identifying **questioned costs*** is issued to FDIC management. Auditors question costs because of an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document governing the expenditure of funds. In addition, a questioned cost may be a finding in which, at the time of the audit, a cost is not supported by adequate

documentation; or, a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

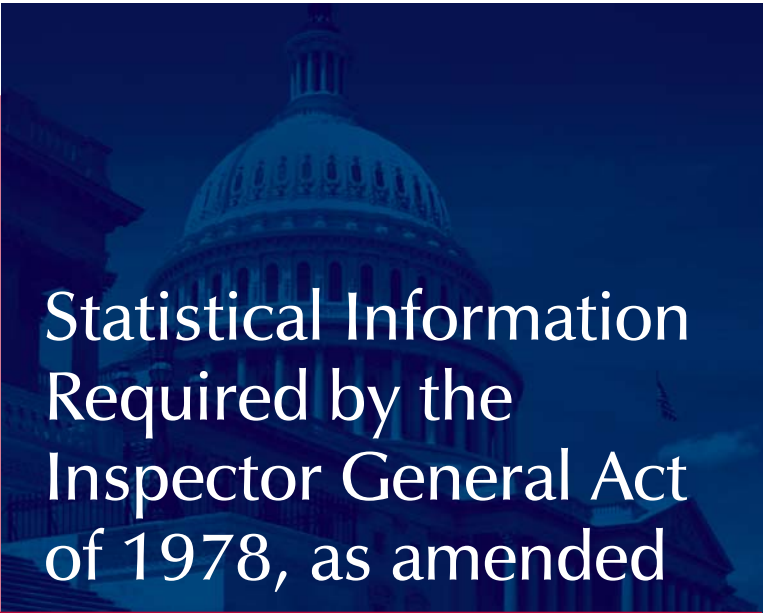
The next step in the process is for FDIC management to make a decision about the questioned costs. The Inspector General Act describes a “**management decision**” as the final decision issued by management after evaluation of the finding(s) and recommendation(s) included in an audit report, including actions deemed to be necessary. In the case of questioned costs, this management decision must specifically address the questioned costs by either disallowing or not disallowing these costs. A “**disallowed cost**,” according to the Inspector General Act, is a questioned cost that management, in a management decision, has sustained or agreed should not be charged to the government.

Once management has disallowed a cost and, in effect, sustained the auditor's questioned costs, the last step in the process takes place which culminates in the “**final action**.” As defined in the Inspector General Act, final action is the completion of all actions that management has determined, via the management decision process, are necessary to

* It is important to note that the OIG does not always expect 100 percent recovery of all costs questioned.

resolve the findings and recommendations included in an audit report. In the case of disallowed costs, management will typically evaluate factors beyond the conditions in the audit report, such as qualitative judgments of value received or the cost to litigate, and decide whether it is in the Corporation's best interest to pursue recovery of the disallowed costs. The Corporation is responsible for reporting the disposition of the disallowed costs, the amounts recovered, and amounts not recovered.

Except for a few key differences, the process for reports with recommendations that **funds be put to better use** is generally the same as the process for reports with questioned costs. The audit report recommends an action that will result in funds to be used more efficiently rather than identifying amounts that may need to be eventually recovered. Consequently, the management decisions and final actions address the implementation of the recommended actions and not the disallowance or recovery of costs.



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

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 the 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 16 recommendations from 7 reports involve improvements in operations and programs. OERM has categorized the status of these recommendations as follows:

Management Action in Process: (16 recommendations from 7 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 04-008 Evaluation of FDIC's Unix Systems Security February 13, 2004	1*	Centralize Unix administration under one Division of Information Resources Management organization. (Note: This Division is now the Division of Information Technology.)
04-009 Evaluation of FDIC's Intrusion Detection and Incident Response Capability February 13, 2004	4	Research and investigate solutions and tools for aggregating event information from different security logging devices to better distinguish malicious activity from normal network traffic to reduce false positives.
04-016 FDIC's Personnel Security Program March 30, 2004	3	Review all employees in moderate risk-level positions to ensure that appropriate background investigations have been performed.
04-028 FDIC's IT Security Risk Management Program – Overall Program Policies and Procedures and the Risk Assessment Process July 30, 2004	1*	Revise FDIC Circular 1310.3 to delineate the FDIC's complete information technology Security Risk Management Program. The revision should be consistent with the National Institute of Standards and Technology Special Publication 800-26 methodology.
05-005 FDIC's Procurement of Administrative Goods and Services January 21, 2005	2*	Develop a performance measurement framework to consistently monitor and periodically report on the procurement process and progress toward achieving goals to improve procurement economy and efficiency.
05-008 FDIC's Supervision of an Institution's Compliance with the Bank Secrecy Act (BSA) March 2, 2005	1	Propose to the Treasury Department and the other primary federal regulators a requirement for institution management to periodically certify the implementation and oversight of the institution's BSA compliance program.
	3*	Require transaction testing in all BSA compliance examinations by expanding the examination documentation module (ED Module) core procedures to include transaction testing.
	4*	Require examiners to perform at least the first two risk-focused BSA examination procedures modules (core and expanded) at FDIC-supervised institutions if any one of a defined set of BSA assessment factors is present.
	5*	Ensure that the adequacy of the BSA compliance program is a key component in the assignment of the management component rating in CAMELS.

*The OIG has not yet evaluated management's actions in response to OIG recommendations.

Table I: Significant Recommendations from Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed *(continued)*

Report Number, Title & Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
	6*	Assess, in conjunction with the other Primary Federal Regulators, the merits of a numeric rating system for BSA compliance, similar to that of other specialty examination areas.
	8*	Develop an internal control process to verify that all BSA violations are promptly included in the systems used to report this information to the Treasury Department.
	11*	Establish procedures, including the use of the Monitoring and Tracking of BSA Problem Institutions list, to eliminate institutions with inadequate BSA compliance programs from consideration for eligibility to bid on franchises or failed bank assets.
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.
	2	Evaluate alternative solutions to augment the current implementation of Entrust/Express for securing sensitive e-mail communications.
	3	Evaluate the feasibility of implementing an e-mail policy compliance tool to achieve greater assurance that sensitive communications are encrypted when appropriate.
	5	Develop a security plan for the e-mail infrastructure that defines the FDIC's security requirements and existing and planned controls for ensuring those requirements are satisfied.

*The OIG has not yet evaluated management's actions in response to OIG recommendations.

Table II: Audit Reports Issued by Subject Area

Audit Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title	Total	Unsupported	
Supervision and Insurance				
05-026 July 15, 2005	Capital Provision Requirements Established Under Supervisory Corrective Actions			
05-027 July 29, 2005	Maximum Efficiency, Risk-focused, Institution Targeted (MERIT) Eligibility Process			
05-038 September 23, 2005	Division of Supervision and Consumer Protection's Risk-focused Compliance Examination Process			
05-039 September 28, 2005	Effectiveness of Supervisory Corrective Actions			
Resolution, Receivership and Legal Affairs				
05-028 August 8, 2005	DRR's Pre-Closing Planning Process			
Information Management				
05-019 June 6, 2005	FDIC's New Financial Environment (NFE) Testing			
05-020 June 9, 2005	Systems and Data Conversion for the New Financial Environment			
05-022 June 15, 2005	Central Data Repository Project Management			
05-037 September 23, 2005	Controls Over the Risk-Related Premium System			
Information Assurance				
05-031 September 8, 2005	FDIC's Information Technology Configuration Management Controls Over Operating System Software			
05-033 September 16, 2005	Response to Privacy Program Information Request in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management			
05-034 September 16, 2005	Responses to Security-Related Questions Raised in OMB's Fiscal Year 2005 Reporting Instructions for FISMA and Agency Privacy Management			
05-040 September 29, 2005	Independent Evaluation of the FDIC's Information Security Program – 2005			

Table II: Audit Reports Issued by Subject Area (continued)

Audit Report		Questioned Costs		Funds Put to Better Use
Number and Date	Title	Total	Unsupported	
Resources Management				
05-018 May 24, 2005	Implementation of E-Government Principles			
EVAL-05-021 June 10, 2005	Status of Virginia Square Phase II Construction			
05-024 June 28, 2005	Inside Board Member and Executive Manager Travel			
05-025 July 14, 2005	FDIC's Investment Policies			
05-029 August 11, 2005	Contract Solicitation and Evaluation			
EVAL-05-032 September 16, 2005	Follow-up Evaluation of the FDIC's Corporate Planning Cycle			
EVAL-05-035 September 21, 2005	FDIC's Corporate University			
EVAL-05-036 September 21, 2005	FDIC's Management of Travel Costs			
Post-award Contract Audits				
05-023 June 24, 2005	Post-award Contract Audit	\$289,463		
05-030 August 25, 2005	Post-award Contract Audit	\$691,892	\$20,000	
Totals for the Period		\$981,355	\$20,000	

Table III: 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.	3	\$354,153	\$47,665
B. Which were issued during the reporting period.	2	\$981,355	\$20,000
Subtotals of A & B	5	\$1,335,508	\$67,665
C. For which a management decision was made during the reporting period.	3	\$354,153	\$47,665
(i) dollar value of disallowed costs.	1	\$675	\$0
(ii) dollar value of costs not disallowed.	3*	\$353,478	\$47,665
D. For which no management decision has been made by the end of the reporting period.	2	\$981,355	\$20,000
Reports for which no management decision was made within 6 months of issuance.	0	\$0	\$0

*One report included on the line for costs not disallowed is also included on the line for costs disallowed because management did not agree with some of the questioned costs.

Table IV: 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.	2	\$361,430
B. Which were issued during the reporting period.	0	\$0
Subtotals of A & B	2	\$361,430
C. For which a management decision was made during the reporting period.	2	\$361,430
(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.	2	\$361,430
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 V: Status of OIG Recommendations Without Management Decisions

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

Table VI: Significant Revised Management Decisions

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

Table VII: Significant Management Decisions with Which the OIG Disagreed

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

Table VIII: Instances Where Information Was Refused

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



Farewell to OIG Retirees



Gary E. Gotherman

Gary Gotherman retired after more than 34 years of federal service. During his many years at the FDIC, he was a constant source of information on the policies and practices of the FDIC OIG as it had

evolved over time. His career at the FDIC included performing liquidation and information technology audits, managing the OIG's earlier internal quality assurance and internal control programs, coordinating issuance of weekly highlight reports to the FDIC Chairman, and preparing the FDIC OIG's first semiannual reports to the Congress. Later, as Deputy Assistant Inspector General for Quality Assurance and Oversight, he provided excellent leadership on a number of important strategic planning, performance measurement, client survey, internal control, and risk management initiatives.



Samuel M. Holland

Samuel Holland retired after serving as Assistant Inspector General for Investigations for 6 years at the FDIC. Under his

direction, the Office of Investigations' nationwide program for the prevention, detection, and investigation of complex, white-collar crimes affecting the FDIC became recognized throughout the federal law enforcement community as a model program, both for the results it achieved and for the effective relationships that Sam forged with the Corporation. Sam served his country for 30 years, initially at the U.S. General Accounting Office where he was an original member of the Office of Special Investigations, and then at the Nuclear Regulatory Commission and Social Security Administration Offices of Inspector General, where he held senior leadership positions. In each professional undertaking, he led, guided, and inspired those with whom he came in contact.

Robert L. McGregor

Robert McGregor retired after more than 32 years of federal service. His federal career began in 1972 at the Department of Labor, where, among other positions, he served as the Director of the Office of Financial Management Audits in the OIG. He also served as the Assistant Inspector General for Oversight and Quality Assurance at the Resolution Trust Corporation



for 5 years. As such, he was responsible for programs and activities related to oversight of the quality of audit, evaluation, and investigative work, including work performed by both the OIG and certified public accountants. Since 1996, Bob served as Assistant Inspector General for Quality Assurance and Oversight at the FDIC where he was responsible for providing leadership, coordination, and oversight of the quality assurance of OIG programs, organizational self-assessments and quality improvement initiatives, client and employee survey initiatives, risk management and internal control activities, and strategic planning and performance measurement activities.



Sharon M. Smith

Sharon Smith retired after more than 31 years of federal service. She had the special distinction of having spent her entire federal career at the FDIC, and in that capacity was a constant source of invaluable

institutional knowledge from which all in the OIG benefited. Sharon began her service in January 1974 as an internal auditor in the Office of Systems and Financial Audits. Over the years she excelled and advanced, eventually becoming a key member of the OIG's senior leadership team. Throughout her tenure at the FDIC, her

expertise, boundless energy, positive attitude, and strong support of accounting and auditing professional organizations inspired her colleagues and attested to her commitment to make the FDIC OIG and the auditing community high-performing and highly effective entities.

Clater J. Sommers

Clater (Jim) Sommers retired after more than 30 years of federal service. During his career, Jim distinguished himself in service to the U.S. Army, Department of Commerce, Air Force Audit Agency, Government Printing Office, Resolution Trust Corporation (RTC), and FDIC. At the RTC and FDIC, Jim's work focused on information technology (IT) issues. His many efforts on audits of the RTC's IT program were instrumental in helping to bring a swift and successful resolution to an unprecedented financial crisis. At the FDIC, his continued focus on IT program issues challenged the Corporation to explore new and innovative approaches to effectively managing major IT projects. Areas he audited included the Year 2000 effort, Time and Attendance Processing System, Corporate Human Resources Management System, and Public Key Infrastructure.





Abbreviations and Acronyms

APM	Acquisition Policy Manual	FBI	Federal Bureau of Investigation
ASTEP	Asset Servicing Technology Enhancement Project	FDIC	Federal Deposit Insurance Corporation
BIF	Bank Insurance Fund	FIAT	Formal and Informal Action Tracking system
BSA	Bank Secrecy Act	FinCEN	Financial Crimes Enforcement Network
CIRC	Capital Investment Review Committee	FISMA	Federal Information Security Management Act of 2002
CPC	Corporate Planning Cycle	FOIA	Freedom of Information Act
CRA	Community Reinvestment Act	FY	Fiscal Year
CU	Corporate University	GSA	General Services Administration
DCSB	Deuel County State Bank	GTR	General Travel Regulations
DOA	Division of Administration	IBM	International Business Machines
DOF	Division of Finance	ILC	industrial loan company
DRR	Division of Resolutions and Receiverships	IRS CID	Internal Revenue Service Criminal Investigation Division
DSC	Division of Supervision and Consumer Protection	IT	Information Technology
ECU	Electronic Crimes Unit	MAS	Multiple Award Schedule
EM	Executive Managers		

MERIT	Maximum Efficiency, Risk-focused, Institution Targeted Examination Program	RRPS	Risk-Related Premium System
NFE	New Financial Environment	SAIF	Savings Association Insurance Fund
NIH FCU	National Institutes of Health Federal Credit Union	SatoTravel	Scheduled Airlines Traffic Offices, Inc.
OC	Office of Counsel	SCS	San Clemente Securities, Inc.
OERM	Office of Enterprise Risk Management	SFG	Stevens Financial Group
OI	Office of Investigations	T&C Bank	Town & Country Bank of Almelund
OIG	Office of Inspector General	T&D	training and development
OMB	Office of Management and Budget	UCC	United Custodial Corporation
PCA	Prompt Corrective Action	USA PATRIOT Act	United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
PCIE	President's Council on Integrity and Efficiency		
PMA	President's Management Agenda		
PwC	PricewaterhouseCoopers, LLC		