



Semiannual Report to Congress

October 1, 2004 – March 31, 2005

OIG

Office of Inspector General



Semiannual Report to Congress

October 1, 2004 – March 31, 2005

OIG

Office of Inspector General



BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

April 22, 2005

The Honorable Alan Greenspan
Chairman
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Chairman Greenspan:

We are pleased to present our *Semiannual Report to Congress* which summarizes the activities of our office for the reporting period October 1, 2004, through March 31, 2005. The Inspector General Act requires that you transmit this report to the appropriate committees of Congress within thirty days of receipt, together with a separate management report and any comments you wish to make.

Sincerely,

/signed/

Barry R. Snyder
Inspector General

Enclosure



Semiannual Report to Congress

October 1, 2004 – March 31, 2005

OIG

Office of Inspector General

Table of Contents

	Page
Introduction.....	1
Goals and Objectives	3
Projects Completed during this Reporting Period	4
Ongoing Projects.....	14
Follow-up Activities	17
Appendixes	21
Appendix 1—Audit Reports Issued with Questioned Costs for the Period October 1, 2004, through March 31, 2005	23
Appendix 2—Audit Reports Issued with Recommendations that Funds be Put to Better Use for the Period October 1, 2004, through March 31, 2005.....	24
Appendix 3—OIG Reports with Outstanding Recommendations.....	25
Appendix 4—Cross-References to the Inspector General Act	26

Introduction

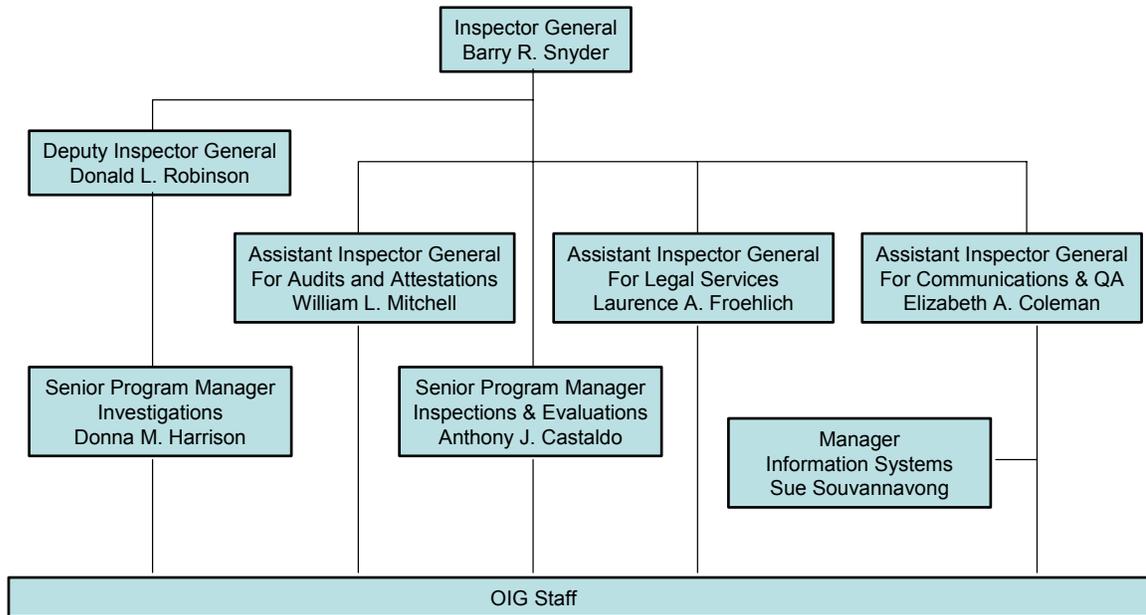
Consistent with the Inspector General Act of 1978 (IG Act), as amended, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- conduct and supervise independent and objective audits, investigations, and other reviews of Board programs and operations;
- promote economy, efficiency, and effectiveness within the Board;
- help prevent and detect fraud, waste, and mismanagement in the Board's programs and operations;
- review existing and proposed legislation and regulations and make recommendations regarding possible improvements to the Board's programs and operations; and
- keep the Chairman and Congress fully and currently informed of problems.

Congress has also mandated additional responsibilities that impact where the OIG directs its resources. For example, section 38(k) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. 1831o(k), requires the Board's OIG to review failed financial institutions supervised by the Board that result in a material loss to the bank insurance funds, and to produce, within six months of the loss, a report that includes possible suggestions for improvement in the Board's banking supervision practices. In the information technology arena, the Federal Information Security Management Act of 2002 (FISMA), Title III of Public Law 107-347, provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. Consistent with FISMA's requirements, we perform an annual independent evaluation of the Board's information security program and practices to include evaluating the effectiveness of security controls and techniques for selected information systems.

OFFICE OF INSPECTOR GENERAL

April 2005

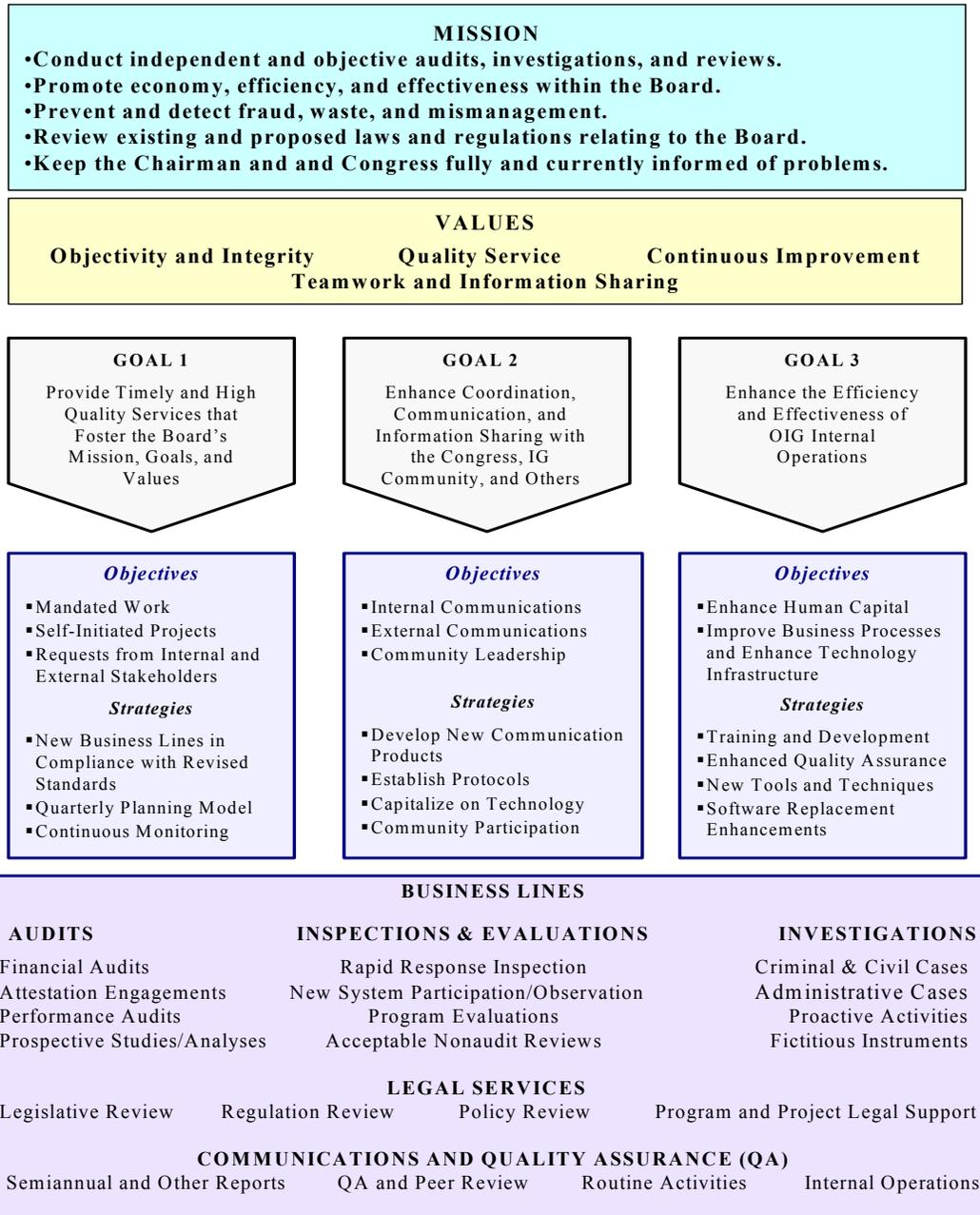


OIG Staffing	
Auditors.....	15
EDP Auditors.....	5
Investigators.....	5
Attorneys	2
Administrative	2
Information Systems Analysts	<u>2</u>
Total Positions	31

Goals and Objectives

The OIG has identified three strategic goals and developed corresponding objectives to guide our work over the next four years. For each strategic goal, we have also identified specific strategies to help achieve the underlying objectives. The exhibit below depicts the relationship of the various elements of our strategic plan, within the context of our mission and values.

Overview of the OIG's Strategic Plan, 2005- 2008



Projects Completed during this Reporting Period

Audit of the Board's Automated Travel System

We began this audit in late 2003 based on user concerns that the Board's new automated travel system, implemented in early 2003, did not meet Board staff expectations and was difficult to use. Our audit objectives were to evaluate the continued viability of the automated system as part of the Board's travel administration process, identify opportunities to improve the efficiency and effectiveness of future system implementations, and follow up on our 1997 *Report on the Business Process Review of Travel Administration*. Shortly after we began our fieldwork, a review team, established by the Staff Director for Management, recommended discontinuing use of the new automated system. The Board's Committee on Board Affairs (CBA) accepted the review team's recommendation and the system was officially discontinued in February 2004.

Overall, our audit found that the new automated travel system was a technically viable solution to the Board's travel administration requirements and we believe that the decision to discontinue the system after less than a year of operation was premature. The system offered several significant benefits to the Board (such as split payments between the user and the government travel card), facilitated document processing, and enhanced controls over travel expenditures. Furthermore, the review committee's recommendation to discontinue the system—based on user concerns, the expected system enhancement cost to address those concerns, and the belief that the system failed to deliver expected cost saving—was based on a limited period of system usage and incomplete cost information.

The decision to discontinue the system has resulted in a hybrid approach to travel administration. We found that most divisions now prepare paper travel authorizations and vouchers which the Management Division (MGT) staff manually enter into the automated system. Some divisions, however, continue to use the system, at least in a limited capacity, for processing travel documents. We are concerned that this hybrid approach to handling travel administration is inefficient and increases the possibility of errors through duplicate data entry. Returning to a paper-based process is also inconsistent with current e-government initiatives and the Board's own objectives to reduce reliance on paper. Nevertheless, we did not recommend that the Board reinstitute the system, given that (1) staff resistance would likely outweigh any efficiencies that would be gained by such a change, and (2) the director of MGT has established two new evaluation groups to set requirements for the Board's travel administration process and develop an easy-to-use system that meets those requirements.

Our audit also identified specific areas in the system implementation process that we believe contributed to user concerns and the lack of Boardwide acceptance. Specifically, the project was not managed under a formal system life cycle methodology, user involvement was lacking, and system training was insufficient. Our report contains three recommendations designed to address these issues. Further, our review of the automated system contract and related documentation

showed that the Board paid the software vendor for services not received and we issued a fourth recommendation that the Board seek reimbursement. Towards that end, we have classified the \$62,700 paid for these services as questioned costs. Finally, our follow-up work on the status of action items from our 1997 business process review report showed that sufficient actions have been taken to close five of the eight open items (see “Follow-Up Activities,” page 17).

We provided our report to the Staff Director for Management for comment. The Staff Director concurred with, and took actions to address, the three recommendations pertaining to the system implementation process. The Staff Director referred our fourth finding to the Legal Division (Legal) for review and guidance on whether the Board should seek reimbursement for services not received. Legal concluded that the Board would be unlikely to recover any contract damages from the software vendor and recommended that the Board not pursue a claim.

Audits of the Board's and the Federal Financial Institutions Examination Council's (FFIEC) Financial Statements for the Year Ended December 31, 2004

Each year, we contract for an independent public accounting firm to audit the financial statements of the Board and the Federal Financial Institutions Examination Council (FFIEC); the Board performs the accounting function for the FFIEC. KPMG LLP, our current contract auditors, planned and performed the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. The audits included examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. The audits also included an assessment of the accounting principles used and significant estimates made by management, as well as an evaluation of overall financial statement presentation. In the auditors' opinion, the Board's and FFIEC's financial statements present fairly, in all material respects, the financial position of each as of December 31, 2004, and the results of operations, and cash flows for the year then ended, in conformity with accounting principles generally accepted in the United States of America.

To determine the auditing procedures needed to express an opinion on the financial statements, the auditors considered the Board's and the FFIEC's internal controls over financial reporting. Although the auditors' consideration of the internal controls would not necessarily disclose all matters that might be material weaknesses, they noted no such matters. As part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, the auditors also performed tests of the Board's and the FFIEC's compliance with certain provisions of laws and regulations, since noncompliance with these provision could have a direct and material effect on the determination of the financial statement amounts. The results of the auditors' tests disclosed no

instances of noncompliance required to be reported under *Government Auditing Standards*.

Review of the Workers' Compensation Program

During this reporting period, we completed our Review of the Board's Workers' Compensation Program (Program). The Board's employees are covered by the Federal Employees' Compensation Act, which pays workers' compensation benefits to federal civilian government employees for disability due to personal injury or occupational disease sustained while in the performance of duty. We performed this review because of recent changes in the staffing and organizational placement of the Program, and because the substantial growth in the size of the Board's guard force, and the nature of their work, increases the Board's risk for additional workers' compensation claims.

As part of our review, we inspected thirty-four workers' compensation cases that were active as of March 31, 2004. We found that the Board fulfilled its responsibilities as outlined in guidelines issued by the Department of Labor. In each case, the appropriate workers' compensation forms were prepared and submitted within the prescribed timeframes.

We also evaluated the Program's overall performance and operations, and found that the Board's workers' compensation expenses compare favorably to other federal agencies and private entities. For example, the Board's 2003 workers' compensation expenses were approximately \$400,000, or .25 percent of total payroll expenses. In contrast, the 2003 workers' compensation expenses of the federal government and the private sector were significantly higher percentages of payroll, at approximately 1.8 and 2.3 percent respectively.

Notwithstanding the Board's relatively low workers' compensation expenses, we made recommendations designed to augment the Program's performance. Specifically, we recommended that the director of MGT establish a "return-to-work" program for worker compensation beneficiaries. Our research revealed that a systematic effort to contact and encourage injured employees to return to work as soon as medically feasible is an industry best practice. Moreover, studies show that early and sustained follow-up emphasizing the availability of modified or light-duty assignments deters claims for long-term disability, and generally reduces overall workers' compensation costs. We also recommended that the director establish a formal process to collect and analyze detailed, Boardwide, accident-related data to identify accident/injury trends. We found that effective workers' compensation programs discern workplace-related injury and illness patterns by employing an ongoing, data-driven process to analyze elements of workers' compensation claims. This analysis can also reveal systemic health and safety weaknesses that, once identified, should be corrected to prevent further work-related injuries.

Our research also showed that fraud is an enterprise-wide risk that can be mitigated by systematically reviewing workers' compensation cases for "red flags" indicating the potential for fraud. Accordingly, we recommended that the director establish an internal control procedure to ensure that workers' compensation cases are systematically reviewed for fraud indicators, and, when appropriate, are referred for further investigation. As part of our review, we developed a fraud indicator worksheet based on a variety of similar instruments being used in public and private sector workers' compensation programs, and prepared worksheets for the workers' compensation cases reviewed during our compliance inspection. Our analysis surfaced three cases that we believe require further scrutiny, and we have referred them to our investigators to determine if any formal investigations are warranted.

Finally, we identified a number of operational issues that should be addressed to improve the Program's overall management and recommended that the director enhance the Program's operations by:

- preparing a job description for the workers' compensation coordinator,
- providing additional training opportunities for the coordinator,
- assigning a backup for the coordinator and ensuring that this employee has sufficient workers' compensation training and program knowledge, and
- preparing written guidance to help Board supervisors fulfill their key role in reporting the facts of an injury and assisting with ongoing case management.

The director of MGT agreed with our conclusions and agreed to implement each of our recommendations.

Review of FFIEC's Call Modernization Project

During this period, we initiated a review of FFIEC's Call Modernization Project at the request of Board senior management. Call Reports are the consolidated reports of financial condition and income filed quarterly by every national bank, state member bank, and insured state nonmember bank. The modernization effort involves designing a new system to improve the processes for collecting, validating, storing, and distributing Call Report information. While the FFIEC is overseeing the entire project, the Federal Deposit Insurance Corporation (FDIC) is responsible for project management, and is working closely with staff from the Federal Reserve System and the Office of the Comptroller of the Currency. The original system implementation date of October 2004 was not met, and is now set for October 2005. After evaluating the issues related to the project delays, we briefed senior Board management on our assessment of project management and technology risks that could affect success in achieving the revised milestone. We will continue monitoring the project's status during the next period.

Audit of the Board's Information Security Program

FISMA requires each agency's Inspector General (IG) to perform an annual independent evaluation of their agency's information security program and practices. The evaluations are designed to test the effectiveness of controls and techniques for a representative subset of the agency's information systems and to assess compliance with the requirements of FISMA. During our 2004 audit of the Board's information security program pursuant to FISMA's requirements, we evaluated the effectiveness of security controls and techniques for three Board applications. Our tests did not identify any significant deficiencies, although we found several areas where controls could be strengthened. Given the sensitivity of the issues involved, we provided the results to management under separate restricted covers. Management agreed with our recommendations and has implemented corrective actions. We will follow up on our recommendations as part of our future information security audit activities.

Review of Configuration Management

FISMA assigned the responsibility for establishing governmentwide policies for the management of information security programs to the director of the Office of Management and Budget (OMB). As part of this responsibility, OMB issued memorandum M-04-25 in August 2004 to assist agencies in fulfilling their FISMA evaluation and reporting responsibilities. M-04-25 required each OIG to report on specific security-related performance measures, including whether the agency's Chief Information Officer (CIO) has implemented agencywide policies that require detailed specific security configurations and the degree to which the configurations are implemented. To accomplish this reporting requirement, we obtained security settings for selected categories of hardware such as servers, workstations, and routers from staff in the Division of Information Technology (IT). We then compared the actual settings used in production against the information provided by IT staff for a judgmental sample of devices maintained by IT and the Division of Research and Statistics. We did not evaluate the appropriateness of the settings as part of this review.

Based on our fieldwork, we provided a restricted management report to the Board's CIO for review and comment. Our report contains four recommendations designed to address the Board's security configuration setting process and related procedures. Although the CIO's initial written response indicated disagreement with several of our recommendations and the underlying issues, we note that the Board's Information Security Committee has initiated actions to address our three recommendations specifically related to configuration management. We will continue to review actions taken in this area during future FISMA audit work.

Investigative Activity

During the reporting period, we opened nine formal investigations and continued work on eight cases that were opened during previous reporting periods. Of our seventeen active cases, we have closed five. The following are highlights of our significant investigative accomplishments:

- **Misuse of fraudulent social security numbers to obtain government documents and establish bank accounts at institutions regulated by the Federal Reserve System.** Pursuant to a search/arrest warrant executed in an OIG joint investigation with the Social Security Administration OIG and the Coast Guard Investigation Service, the subject of this investigation pleaded guilty to a one-count violation of 18 U.S.C. 1001(a)(2) (False Statements) and a two-count violation of 42 U.S.C. 408(a)(7)(A) (Misuse of Social Security Account Number). The subject was released on \$5,000 unsecured bond, and sentencing is pending.
- **Bank fraud and money laundering allegations.** The OIG participated in a joint investigation with the Drug Enforcement Administration (DEA) to determine whether targets of a specific DEA investigation were involved in bank fraud and money laundering activities. The OIG coordinated with the Board's Division of Banking Supervision and Regulation (BS&R) to facilitate a review of the subject's background and involvement with depository institutions. The review did not substantiate specific evidence of money laundering or other criminal activity. As a result of OIG's effort in this case, the DEA was able to close their case.
- **Telephonic death threat to Board employee.** The OIG conducted an investigation involving a specific death threat left on a Board employee's voice mail message account. OIG investigators identified several juvenile suspects, one of whom made admissions regarding his role in placing the threatening telephone call to the Board employee. The case was referred to the U.S Attorney for prosecution and the matter was declined in favor of alternative remedies since the offender was a juvenile. OIG investigators cautioned the juvenile and his parent regarding the criminal nature of the threatening telephone call and warned that further such calls could result in criminal prosecution.
- **"Diploma Mill Degree" abuse allegations.** The OIG conducted an investigation as a result of a U.S. Government Accountability Office (GAO) referral alleging that a Board employee utilized an advanced degree obtained from an unaccredited university to obtain a Board position, promotion and/or degree-associated reimbursement. The investigation substantiated allegations that the employee did have an advanced degree from an unaccredited university. It was also determined, however, that this employee did not receive any benefit from the Board as a result of his

diploma mill degree. The results of this investigation were reported to GAO and Board management.

At the end of this reporting period, we had twelve active cases. Our summary statistics on investigations are provided in the table that follows:

Summary Statistics on Investigations for the Period October 1, 2004, through March 31, 2005

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	9
Investigations Open from Previous Period	8
Investigations Closed during Reporting Period	5
Total Investigations Active at End of Reporting Period	12
Investigative Results for this Period	
Referred to Prosecutor	1
Referred for Audit	0
Referred for Administrative Action	0
Oral and/or Written Reprimand	0
Terminations of Employment	0
Suspensions	0
Debarments	0
Indictments	0
Convictions	1
Monetary Recoveries	\$0
Civil Actions (Fines and Restitution)	\$0
Criminal Fines: Fines & Restitution	\$0

Hotline Operations

Our investigators continue to address allegations of wrongdoing related to the Board’s programs and operations, as well as violations of the Board’s standards of conduct. During this reporting period, we received 117 complaints, of which ninety-seven were from our hotline operation. Most hotline callers were consumers with complaints or questions about practices of private financial institutions. Those inquiries involved matters such as funds availability, account fees and charges, and accuracy and availability of account records. We also continued to receive numerous questions concerning how to process Treasury securities and savings bonds. Other callers contacted us seeking advice about programs and operations of the Board, Federal Reserve Banks, other OIGs, and other financial regulatory agencies. We directed those inquiries to the appropriate Board offices, Reserve Banks, or federal or state agencies. We closed all but ten of the ninety-seven hotline complaints after our initial analysis and contact with the complainants.

In addition to the hotline complaints, the investigative services program received a total of twenty allegations: eleven from Board program staff, six from other sources, and three from OIG audit staff. As a result of those allegations, the OIG opened nine investigations. In addition, we are continuing our review of fictitious

instrument fraud complaints. Fictitious instrument fraud schemes are those in which promoters promise very high profits based on fictitious instruments that they claim are issued, endorsed, or authorized by the Federal Reserve System or a well-known financial institution.

Our summary statistics of the hotline results are provided in the table that follows:

Summary Statistics on Hotline Results for the Period of October 1, 2004, through March 31, 2005

Investigative Actions	Number
Complaints Referred for Investigation	
Hotline Referrals	97
Audit Referrals	3
Referrals from Other Board Offices	11
Referrals from Other Sources	6
Proactive Efforts by OIG	
Investigations Developed by OIG	0
Results of all Complaints Referred and Proactive Efforts	
Resolved	107
Pending	10
Total Received during Reporting Period	117

Executive Council on Integrity and Efficiency Participation

As Vice Chair of the Executive Council on Integrity and Efficiency (ECIE), the Board’s IG provides leadership, vision, direction, and initiatives for the ECIE on behalf of the Council Chair (the Deputy Director for Management, Office of Management and Budget). Collectively, the members of the ECIE have continued to work with the members of the President’s Council on Integrity and Efficiency (PCIE) to help improve Government programs and operations.

As ECIE Vice Chair, the Board’s IG once again is collaborating with the PCIE in producing *A Progress Report to the President, Fiscal Year 2004*, an annual publication that highlights the collective work and accomplishments of the IG community and the Councils’ progress in achieving strategic goals and objectives. This year, our primary contribution was to gather and consolidate statistical data on thousands of audits, evaluations, and investigations conducted across the IG community. The Councils plan to issue the report early in the next reporting period.

OIG Governance Framework

To continue to build on our information technology infrastructure, the OIG initiated a project to develop a governance framework that encompasses the full range of our work; leverages the capabilities of the new technology in a user-friendly manner; and strengthens and simplifies our policies and procedures. During this reporting period, the OIG completed or refined key policy overview documents and supporting policies and procedures related to direction and communication, human capital management, and project management. The resulting governance framework better positions us to ensure and document compliance with applicable standards, clearly integrate and link written policies and procedures with our day-to-day work, educate internally and externally, and further strengthen and streamline our infrastructure and processes. We plan to continually monitor and update OIG policies as warranted, including operational policies for our internal administration and operations.

Review of Legislation and Regulations

Pursuant to the IG Act, as amended, we review existing and proposed legislative and regulatory items both as part of our routine activities and on an *ad hoc* basis. We routinely track proposed and pending legislation as well as regulations by researching relevant documents and databases, reviewing lists prepared by the Board's law library, sharing information with others in the IG community, and coordinating with Board programs that also review new and proposed legislation. We then independently analyze the effect that the new or proposed legislation or regulations may have on the efficiency and effectiveness of the programs and operations of the Board, including the OIG.

During this reporting period, we reviewed numerous bills on a variety of topics. For example, we reviewed the "Faster FOIA Act of 2005" (S. 589) and the "Openness Promotes Effectiveness on our National Government Act" (OPEN Government Act of 2005, S. 394), both of which are intended to make changes in the way that agencies process requests under the Freedom of Information Act. We also reviewed the "The Terrorist Apprehension and Record Retention Act of 2005" ("The TARR Act of 2005," H.R. 1225) which imposes certain requirements on law enforcement agencies when an individual attempting to obtain a firearm is identified as a known or suspected member of a terrorist organization. Among other bills we reviewed were S. 636 ("A Bill to direct the Inspector General of the Department of Justice to submit semi-annual reports regarding settlements relating to False Claims and Fraud against the Federal Government"); S. 494 ("Federal Employee Protection of Disclosures Act"); and H.R. 185 ("Program Assessment and Results Act").

In addition to proposed legislation, we reviewed several recently-enacted public laws. In particular, we reviewed "The Justice for All Act" (Pub.L. 108-405,

enacted October 30, 2004) which, among other things, assigns to law enforcement agencies—such as the OIG—certain responsibilities toward crime victims arising out of the criminal investigations we conduct. We also reviewed “The Intelligence Reform and Terrorism Prevention Act of 2004” (Pub.L. 108-458, enacted December 17, 2004) which permits the new Director of National Intelligence to establish an OIG.

We also carried out additional work on a variety of topics. For example, we coordinated with Congressional staff and the PCIE’s Legislation Committee as they consider proposed legislation to enhance the operations of the IG community. We also continued to review and analyze the scope and effect of FISMA on Board programs and operations, with particular emphasis on its applicability to Board-related information and systems operated by third parties.

Our review of legislation and regulations also includes commenting on revisions or additions to the Board’s management policy statements and internal administrative procedures. For example, we analyzed and provided comments on proposed updates to the Board’s “Vacant Position Posting Policy.” We also had the opportunity to review, and provided comments on, the draft “Recommendations for the Effective Management of Government Information on the Internet and Other Electronic Records” from the government’s Electronic Records Policy Working Group (coordinated by the National Archives and Records Administration). Our comments focused on streamlining the recommendations and ensuring their consistency with the IG Act.

Ongoing Projects

Audit of the Board's Fixed Asset Management Process

Last year, we began a review of the Board's processes for managing its fixed assets. Our audit objectives are to evaluate controls over the receipt, recording, and disposal of fixed assets for two specific asset accounts: office automation (non-mainframe) computer equipment and office machine/other equipment; determine whether amounts recorded in the Board's general ledger for these two accounts are accurate; identify best practices for conducting, tracking, and recording fixed asset inventories; and evaluate the Board's capitalization policy. As part of this audit, we also conducted a physical inventory of a sample of the Board's fixed assets. We have completed fieldwork and plan to issue our report during the next reporting period.

Review of the Failure of the Bank of Ephraim

On June 25, 2004, the Utah Commissioner of Financial Institutions closed the Bank of Ephraim—a small state member bank headquartered in central Utah. The FDIC estimates that the Bank of Ephraim failure will result in an approximately \$5.4 million loss to the Bank Insurance Fund. The amount of this loss is below the Federal Deposit Insurance Act threshold that requires the OIG to assess a failed institution's supervision. Nevertheless, we decided to perform this review because the Bank of Ephraim failure involved fraud, and the loss constitutes a relatively high percentage of the institution's total assets. The objectives of our review are to analyze the Bank's supervision, ascertain why the institution's problems led to failure, and determine if steps can be taken to prevent any such losses in the future. We plan to issue a report on the Bank of Ephraim failure during the next period.

Inspection of the Board's Guard Force

Section 364 of the USA PATRIOT Act of 2001 established federal law enforcement authority for the Federal Reserve and authorized personnel to act as law enforcement officers and to carry firearms to protect and safeguard the premises, grounds, property, and personnel of the Board or any Federal Reserve Bank. In March 2004, we completed an evaluation of the Board's progress in the initial phase of implementing its federal law enforcement authority and transitioning to an armed security force. Now that the transition is largely completed, we plan to perform an inspection of the Board's guard force. We are currently engaged in a scoping effort to establish an inspection methodology and approach based on industry "best practices."

Ongoing Information Security Work

To help fulfill our independent evaluation responsibilities as required by FISMA, we have undertaken several projects as part of an effort to perform work throughout the year related to information security. Listed below are four projects that were in process at the end of the reporting period.

Review of DB2

As part of our 2004 information security audit, we reviewed the security settings and processes for administering the Board's mainframe database software package (DB2). Our objectives were to assess the adequacy of baseline DB2 security settings, as well as evaluate security controls over user accounts, internal DB2 tables, and selected groups with powerful authority within DB2. To achieve our objectives, we interviewed managers and staff in IT and reviewed applicable policies and procedures. Specifically, we reviewed detailed security settings, the use of encryption to protect sensitive logon IDs and passwords, processes for granting and removing access, audit trails and reports, and access controls over sensitive files from which DB2 executes.

Overall, our review showed that the administration of DB2 and related security settings provides an appropriate level of security. However, we identified several areas where we believe security can be enhanced. We have prepared a management letter containing four suggestions for the Board's CIO and Information Security Officer to consider.

Audit of the Federal Reserve System's Approach to FISMA Compliance for Supervision and Regulation

FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. FISMA requires agencies to provide information security for all agency systems, including systems managed on behalf of the agency by another agency, contractor, or other source. Although the Federal Reserve Banks are not directly subject to FISMA's requirements, information systems that are used or operated by a Reserve Bank on behalf of an agency (such as systems supporting the Board's delegated supervision and regulation function) are subject to the legislation's requirements.

Late last year, we began an audit to evaluate (1) the policies and procedures established by BS&R and IT to ensure that applications owned or operated by Reserve Banks on behalf of the Board meet FISMA

requirements, and (2) the Reserve Bank's implementation of those policies and procedures, focusing on how the Reserve Bank application inventories were complied. During this period we completed our fieldwork and are drafting a report for review and comment by the Board's CIO.

Review of the Board's Implementation of Software Security Reviews

In November 2004, we began a scoping effort of the processes used by the Board for requiring and performing software security reviews (SSRs). We began this project as a result of questions raised during our annual audit of the Board's information security program. During that audit, we noted that the Board's information security program document incorporates procedures for performing SSRs on single purpose software that is used by business functions that have a risk level of moderate or high. Because our audit identified at least one software package for which a review had not been performed, we decided to perform additional work.

We have decided to close this project as a result of information obtained during our scoping effort. We have, however, issued a draft report to the CIO based on our scoping work. We will incorporate the CIO's response into our final report, which we expect to issue during the next period.

Follow-Up Activities

Over the past six months, we have undertaken follow-up work on the outstanding recommendations related to six prior OIG reports. Listed below is a status of our follow-up work, including the recommendations that we have closed and those recommendations where follow-up review work is still in process.

Business Process Review of the Board's Travel Administration

Our 1997 report contained nine action items designed to help the Board reengineer the travel administration processes. Our follow-up work completed in 1999 closed one of those items which allowed senior management at the director level and above to authorize their own travel. As part of our audit of the Board's automated travel system (see the discussion on our *Audit of the Board's Automated Travel System*, page 4), we followed up on the status of the remaining eight action items and found that the Board had taken measures to close five additional items. These five items related to the use of discount airfares, the use of frequent flyer benefits, full implementation of the government travel card program, arranging an electronic data interchange with the contracted travel agency, and implementing an automated notification system to help collect funds due the Board. The three remaining action items related to automating the travel authorization process, automating the expense voucher process, and outsourcing the Board's transportation reservation systems. We will review actions taken on the three remaining items after the Board completes ongoing work related to automating travel administration.

Audit of the Federal Reserve's Background Investigation Process

We have continued to meet with MGT staff regarding actions taken to improve the Board's background investigation program. MGT staff have developed an action plan to enhance the Board's background investigation process for contractors, summer interns, temporary employees, and transferred employees. We believe that the action plan, once implemented, will address our two recommendations in this area, and we will perform additional testing once implementation has been completed. We also found that MGT has updated internal policies regarding the Board's employment security program, but that broader Boardwide guidance has not yet been completed. Updating the guidance, consistent with our original recommendation, is necessary to help provide all employees with an understanding of the Board's background investigation requirements, role and responsibilities, and associated processing procedures.

Audit of the Federal Reserve Board's Government Travel Card Program

Our January 2002 report contained five recommendations designed to help the Board establish and communicate clear guidance on the travel card program and

to improve internal controls over issuing, monitoring, and canceling government travel cards (GTCs). We met with MGT staff to discuss revisions to the Board's "Travel Regulations," as well as changes to MGT's processes related to GTCs. We found that the "Travel Regulations" have been revised to update the list of appropriate and inappropriate GTC use, provide additional detail information regarding the use of the GTC for combined business and personal use, and provide procedures for requesting a change in pre-established GTC credit limits. We also found that there were four intranet articles posted in 2002 related to GTCs and one article in 2003. Although there were no corresponding articles posted in 2004 or thus far in 2005, MGT staff we spoke with seemed committed to ensuring that additional reminders are provided to Board staff. Our follow-up work also showed that MGT has developed internal operating procedures related to GTC processes. The procedures cover a variety of topics, such as credit card applications, credit card reports, limit increases, and closing accounts. Based on the actions taken, we are closing two of our recommendations

Our discussions with MGT staff indicated that procedures have been strengthened consistent with our remaining recommendations related to improving controls over the authorization process, monitoring employee credit card use, and closing accounts. We are still reviewing the relevant documentation provided by MGT staff. We plan to test the list of active cardholders against a list of current employees in the Board's personnel system, as well as a sample of questionable transactions for proper follow-up and retention of supporting documentation. Once this testing is completed, we anticipate closing the remaining recommendations.

Audit of the Board's Security-Related Directed Procurements

Our September 2002 report contained two recommendations designed to strengthen the policies and procedures over unique purchases and a third recommendation related to strengthening controls over payments related to fixed-unit-price service contracts. We met with MGT staff and reviewed changes to the Board's *Acquisition Policy* and to the Procurement Section's internal operating procedures. Our follow-up showed that the *Acquisition Policy* has been revised to strengthen controls over directed procurements by establishing dollar thresholds for approvals by the director of MGT, the Staff Director for Management, and the Administrative Governor. The policy has also been updated to require written justification as well as Legal review for all directed procurements. In addition, MGT's internal acquisition procedures have been updated to reflect changes made to the *Acquisition Policy*. We believe that these actions are sufficient to close our first two recommendations.

Regarding our third recommendation, we understand that training for Contracting Officer's Technical Representatives has been revised to address the issues cited in our recommendation. We are reviewing the changes to the course materials and

will provide management with the results of our analysis early in the next reporting period.

Audit of Retirement Plan Administration

Our July 2003 audit report contained four recommendations describing policy decisions that the Board, either through the CBA or through its representation on other Systemwide oversight committees, needed to make to strengthen oversight and administration of the retirement plan. Last year we closed our recommendation regarding the methodology for allocating benefit-related expenses to the Board and Reserve Banks. Since then, we have conducted additional meetings with staff in MGT and Legal to discuss actions taken on our other recommendations and reviewed related documentation. Regarding our recommendation that the CBA establish clear guidance for the role of MGT staff to support retirement processing, we found that MGT discussed our recommendation with the Administrative Governor and received his endorsement for continuing their current approach. We note, however, that the MGT is working closely with the firm to which most of the retirement plan administration and processing functions have been outsourced to help ensure the proper level of service for Board employees, and that the firm has identified Board plan “specialists.” MGT staff have also committed to reviewing their level of involvement after two years. Based on these actions, we are closing this recommendation.

Regarding our other two recommendations, we found that the methodology for including lump-sum payments in the retirement calculation has been revised and that Board staff are working with the Office of Employee Benefits (OEB) to revise the Retirement Plan documents to reflect this change. We plan to test a small sample of recent retirees to verify the processing changes and anticipate closing this recommendation in the next quarter. To address our final recommendation regarding the establishment of an audit committee, Board staff discussed this issue with Board and System officials (including several of the Governors) who seemed satisfied with the current level of oversight. None of these officials favored the creation of another oversight committee. Nevertheless, a member of the Committee on Plan Administration (CPA)--which has primary oversight responsibility for the audit function of OEB and the retirement plan and assets--indicated that the CPA has committed to providing greater coordination of audit matters with the other retirement plan committees and that the CPA charter has been revised to reflect this higher level of coordination. We plan to review the revised committee charter and anticipate closing this recommendation once our review is complete.

Audit of the Board's Automated Travel System

Our November 2004 audit report contained three recommendations designed to address issues related to project management, user involvement, and system training. Our report also contained a fourth recommendation related to the automated system contract and related documentation; specifically, we found that the Board paid the software vendor for services not received and we recommended that the Board seek reimbursement. Earlier this year, Legal reviewed the potential for bringing a legal action against the vendor in connection with this payment and concluded that the Board would be unlikely to recover any contract damages. Legal therefore recommended against pursuing a claim. Given this conclusion, we are closing our recommendation. We will review actions taken on the three remaining recommendations after the Board completes ongoing work related to automating travel administration.

Appendix

Appendix 1
Audit Reports Issued with Questioned Costs for the Period October 1, 2004,
through March 31, 2005

Reports	Number	Dollar Value	
		Questioned Costs	Unsupported
For which no management decision had been made by the commencement of the reporting period	0	\$0	\$0
That were issued during the reporting period	1	\$62,700	\$0
For which a management decision was made during the reporting period	1	\$62,700	\$0
(i) dollar value of disallowed costs	0	\$0	\$0
(ii) dollar value of costs not disallowed	1	\$62,700	\$0
For which no management decision had been made by the end of the reporting period	0	\$0	\$0
For which no management decision was made within six months of issuance	0	\$0	\$0

Appendix 2
Audit Reports Issued with Recommendations that Funds be Put to Better Use
for the Period October 1, 2004, through March 31, 2005

Reports	Number	Dollar Value
For which no management decision had been made by the commencement of the reporting period	0	\$0
That were issued during the reporting period	0	\$0
For which a management decision was made during the reporting period	0	\$0
(i) dollar value of recommendations that were agreed to by management	0	\$0
(ii) dollar value of recommendations that were not agreed to by management	0	\$0
For which no management decision had been made by the end of the reporting period	0	\$0
For which no management decision was made within six months of issuance	0	\$0

Appendix 3

OIG Reports with Outstanding Recommendations

Projects Currently Being Tracked	Issue Date	Recommendations			Status of Recommendations ¹		
		No.	Mgmt. Agrees	Mgmt. Disagrees	Follow-up Completion Date	Closed	Open
Business Process Review of the Board's Travel Administration	07/97	9	9	0	11/04	6	3
Audit of the Board's Efforts to Implement Performance Management Principles Consistent with the Results Act	07/01	4	4	0	08/03	0	4
Audit of the Federal Reserve's Background Investigation Process	10/01	3	3	0	04/04	0	3
Audit of the Federal Reserve Board's Government Travel Card Program	01/02	5	5	0	03/05	2	3
Audit of the Board's Security-Related Directed Procurements	09/02	3	2	1	03/05	2	1
Audit of Retirement Plan Administration	07/03	4	3	1	03/05	2	2
Audit of the Board's Outsourcing Operations	04/04	3	3	0	–	–	–
Review of the Fine Arts Program	04/04	2	2	0	–	–	–
Effectiveness of Administrative Controls Over an Outsourced Contract	06/04	2	2	0	–	–	–
Audit of the Board's Information Security Program	09/04	5	5	0	–	–	–
Audit of the Board's Automated Travel System	11/04	4	4	0	02/05	1	3
Review of the Board's Workers' Compensation Program	03/05	4	4	0	–	–	–

¹ A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable, or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the Board is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred it to the appropriate oversight committee or administrator for a final decision.

Appendix 4

Cross-References to the Inspector General Act

Indexed below are the reporting requirements prescribed by the Inspector General Act of 1978, as amended, for the reporting period:

Section	Source	Page(s)
4(a)(2)	Review of legislation and regulations	12
5(a)(1)	Significant problems, abuses, and deficiencies	None
5(a)(2)	Recommendations with respect to significant problems	None
5(a)(3)	Significant recommendations described in previous Semiannual Reports on which corrective action has not been completed	None
5(a)(4)	Matters referred to prosecutory authorities	10
5(a)(5)	Summary of instances where information was refused	None
5(a)(6)	List of audit reports	4-8
5(a)(7)	Summary of significant reports	None
5(a)(8)	Statistical Table—Questioned Costs	23
5(a)(9)	Statistical Table—Recommendations that Funds Be Put to Better Use	24
5(a)(10)	Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made	25
5(a)(11)	Significant revised management decisions made during the reporting period	None
5(a)(12)	Significant management decisions with which the Inspector General is in disagreement	None



*Inspector General Hotline
1-202-452-6400
1-800-827-3340*

*Report: Fraud, Waste or Mismanagement
Information is confidential
Caller can remain anonymous*

*You may also write the:
Office of Inspector General
HOTLINE
Mail Stop 300
Board of Governors of the Federal Reserve System
Washington, DC 20551*

