



Semiannual Report to Congress

April 1 – September 30, 2006

OIG

Office of Inspector General



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

OFFICE OF INSPECTOR GENERAL

October 31, 2006

The Honorable Ben S. Bernanke
Chairman
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Chairman Bernanke:

We are pleased to present our *Semiannual Report to Congress* which summarizes the activities of our office for the reporting period April 1 through September 30, 2006. 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

April 1 – September 30, 2006

OIG

Office of Inspector General

Table of Contents

	Page
Introduction.....	1
Goals and Objectives	3
Audits and Attestations.....	4
Inspections and Evaluations.....	8
Investigations	9
Legal Services.....	12
Community Participation and Internal Operations	14
Appendixes	17
Appendix 1—Audit Reports Issued with Questioned Costs for the Period April 1 through September 30, 2006	19
Appendix 2—Audit Reports Issued with Recommendations that Funds be Put to Better Use for the Period April 1 through September 30, 2006.....	20
Appendix 3—OIG Reports with Outstanding Recommendations.....	21
Appendix 4—Cross-References to the Inspector General Act	22

Introduction

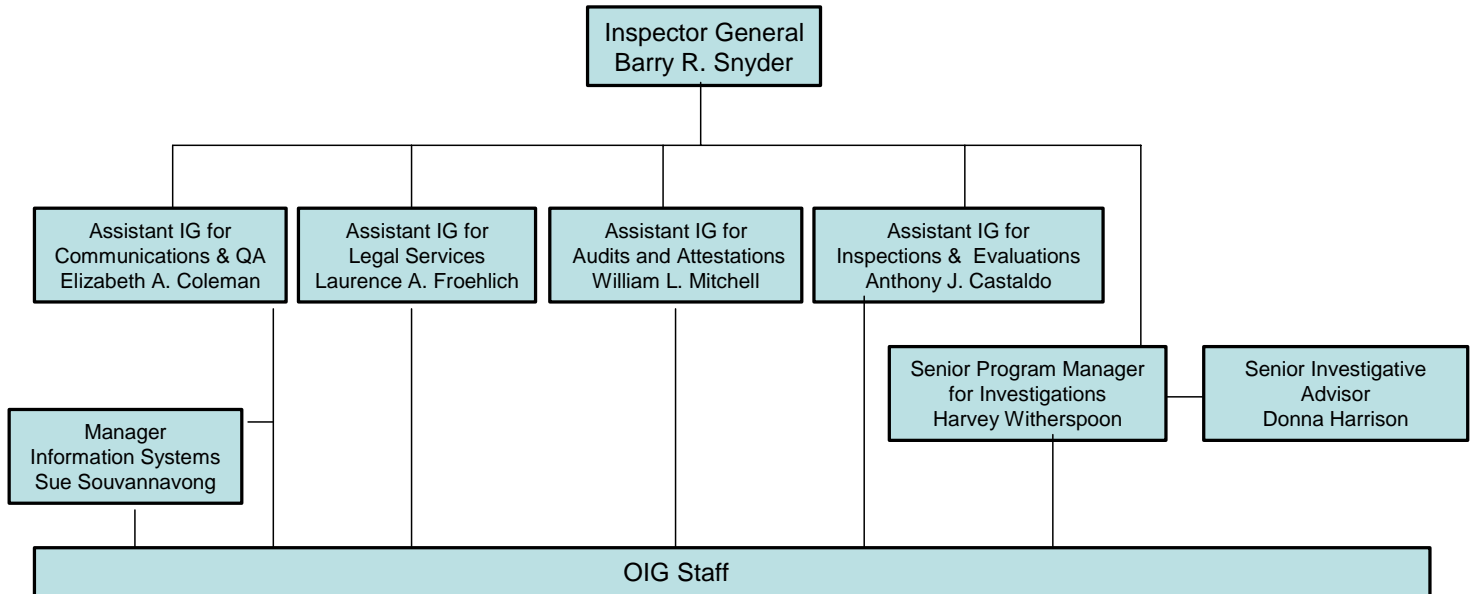
Consistent with the Inspector General Act of 1978 (IG Act), as amended, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- 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, which includes evaluating the effectiveness of security controls and techniques for selected information systems.

OFFICE OF INSPECTOR GENERAL

May 2006

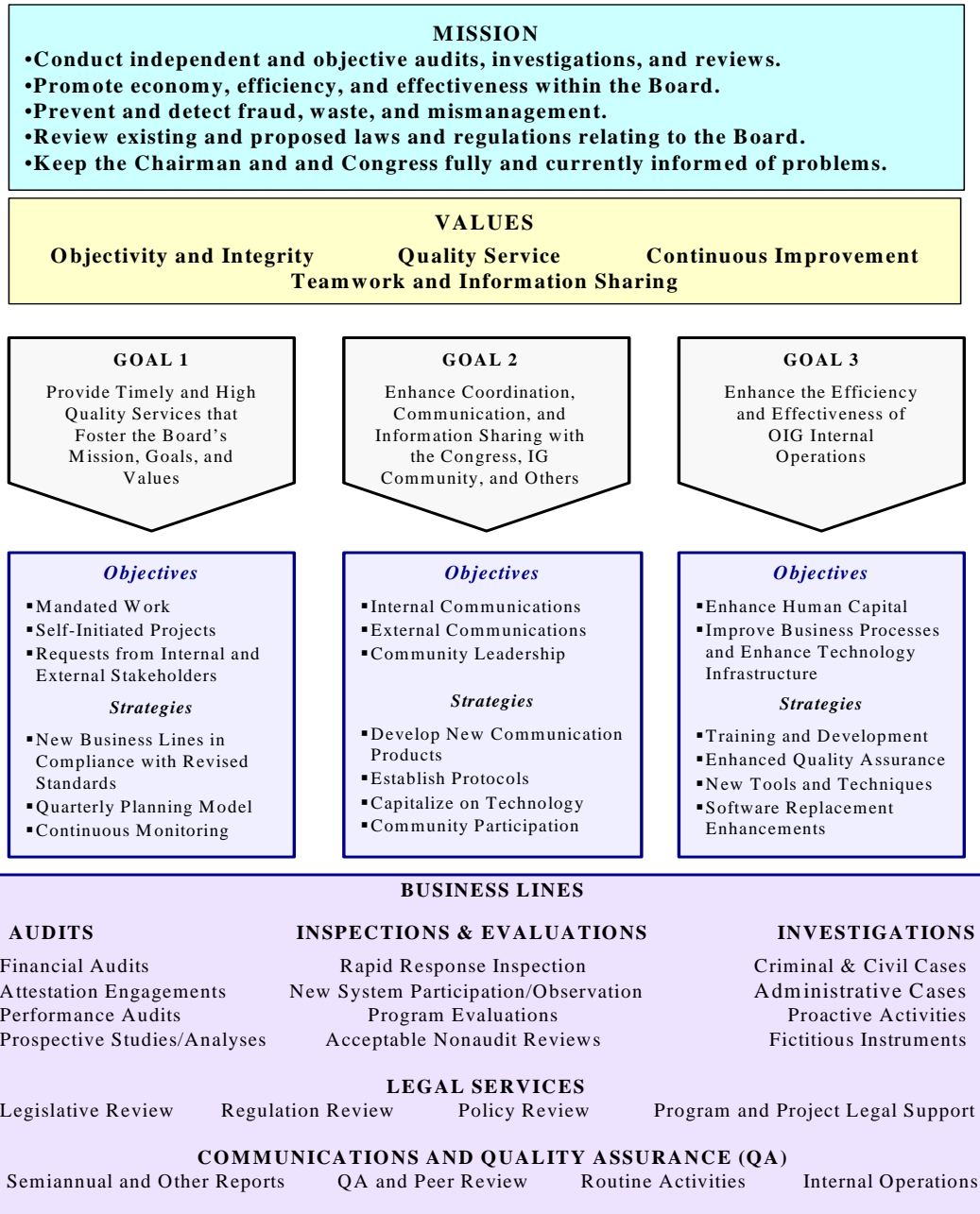


OIG Staffing	
Auditors	17
IT Auditors	6
Investigators	5
Attorneys.....	2
Administrative.....	2
Information Systems Analysts.....	3
Total Authorized Positions	35

Goals and Objectives

The OIG has identified three strategic goals and developed corresponding objectives to guide our work through 2008. For each strategic goal, we have also identified specific strategies to help achieve the underlying objectives. The diagram 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



Audits and Attestations

The OIG's audit and attestation activities are designed to evaluate or examine certain aspects of the economy, efficiency, and overall effectiveness of the Board's programs and operations; the presentation and accuracy of the Board's financial statements, budget data, and financial performance reports; the effectiveness of internal controls governing the Board's contracts and procurement activities; the adequacy of controls and security measures governing the Board's financial and management information systems and the safeguarding of the Board's assets and sensitive information; and the degree of compliance with applicable laws and regulations related to the Board's financial, administrative, and program operations. The information below summarizes our work completed during the period, including our follow-up activities.

Audit of the Board's Financial Statements for the Year Ended December 31, 2005

Each year, we contract for an independent public accounting firm to audit the financial statements of the Board. KPMG LLP, our current contracted auditors, planned and performed the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. The audit included examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. The audit 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.

During the reporting period, the auditors completed fieldwork related to the Board audit and issued the audit report. In the auditors' opinion, the Board's financial statements present fairly, in all material respects, the financial position of the Board as of December 31, 2005; and the results of its operations, and its 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 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. However, the auditors noted certain matters over financial reporting and its operations that they considered to be a reportable condition. These matters related to controls over accounts payable and accrued liabilities, as well as controls over the census data used by the Board's actuary in the pension benefit liability calculation.

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 compliance with certain provisions of laws and regulations, since noncompliance with these provisions 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*.

Audit of the Board's Information Security Program

We performed our audit pursuant to the requirement of FISMA that each agency Inspector General (IG) conduct an annual independent evaluation of the agency's information security program and practices. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate compliance by the Board with FISMA and related information security policies, procedures, standards, and guidelines.

To evaluate security controls and techniques, we reviewed controls over two applications and followed up on the open issue from our 2005 application control review. We performed our 2006 application control testing based on controls identified in the National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (SP 800-53). The SP 800-53 controls are divided into seventeen "families" (such as access controls, risk assessment, and personnel security) and include controls that can be categorized as system-specific or common (i.e., applicable across agency systems). As a result, although our focus was on evaluating specific applications, we also assessed many of the broader organizational security controls that impact most, if not all, applications. One of the applications we reviewed is a supervision and regulation (S&R) system maintained at the Board. We also reviewed a system maintained by the Federal Reserve Bank of New York (FRB NY) in support of the Board's statistical reporting function.

Our control tests identified areas where controls need to be strengthened. Because some of the issues we identified are more significant—either alone or in combination with other weaknesses—we classified several of our findings as "control deficiencies." We also found that FRB NY had not yet implemented any of the processes associated with the Board's revised information security program for the application we reviewed; these processes are fundamental FISMA requirements. Given the sensitivity of the issues involved with these reviews, we are providing the specific results to management in separate restricted reports. Follow-up work on our 2005 application control review allowed us to close the outstanding recommendation.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations in our 2004 and 2005 information security audit reports issued pursuant to FISMA's requirements. Because FISMA authorizes the IGs to base their annual evaluation in whole or in

part on existing audits, evaluations, or reports relating to programs or practices of the agency, we also incorporated the results from, and actions taken on, (1) our 2005 audit of efforts by the Federal Reserve System to implement FISMA's requirements for applications operated by the Reserve Banks in support of the Board's delegated S&R function and (2) our 2006 audit report related to electronic authentication.

In addition, we compiled information on, and reviewed the Board's processes related to, areas for which the Office of Management and Budget (OMB) requests a specific response as part of the agency's annual FISMA reporting. Areas we reviewed include security awareness and training, certification and accreditation (C&A), remedial action monitoring, incident response, and configuration management. Our work on configuration management identified issues related to the Board's processes for establishing, implementing, and maintaining baseline configurations that we will report separately to management. We also compiled information on controls planned or in place related to personally identifiable information which we separately reported to OMB through the IG community.

Overall, we found that the Board's information security program continues to evolve and mature. Our work showed that, over the past year, the Board has made considerable progress toward implementing a structured information security program as outlined by FISMA and has taken actions to address open audit recommendations. Specifically, we found that the Board has developed additional program guidance, revised its application inventory, begun C&A work, and incorporated the Reserve Bank S&R applications into the revised security program. However, the Board still has work remaining to fully implement recent NIST guidance, as well as all aspects of the Board's revised security program. Consequently, several of our audit recommendations remain open. Based on our audit fieldwork, we also provided two additional recommendations related to training on the Board's new information security program and to training staff with significant security responsibilities. In her response to our audit report, the director of the Division of Information Technology, who serves as the Board's Chief Information Officer for FISMA, agreed to implement our audit recommendations. The director also cited several efforts the Board has undertaken to protect its systems from malicious software, unauthorized use, and growing threats. We will follow-up on actions taken regarding our recommendations as part of future audit and evaluation work related to information security.

Follow-up of the Report on the Business Process Review of the Board's Travel Administration and the Report on the Audit of the Board's Automated Travel System

Over the past six months, we have completed follow-up work and closed all outstanding recommendations related to our July 1997 *Business Process Review*

of the Board's Travel Administration and our November 2004 *Report on the Audit of the Board's Automated Travel System*. Actions taken by the Board related to travel administration and automation include:

- The Board has consolidated all of its travel reservation services with SATO Travel, thus discontinuing the use of an in-house reservations desk. This action allows us to close our related 1997 recommendation to outsource that function.
- The Board's automated travel system is being used by Management Division (MGT) staff to process travel expense statements and some divisions are using it to submit expense statements electronically. While our 1997 report envisioned a more robust, Boardwide use of automation for processing travel authorizations and expense statements, we recognize that the current level of automation is the likely status quo for the foreseeable future, and therefore, we have decided to close our remaining recommendations from the 1997 report. Given the continued emphasis on electronic government initiatives, we will continue to review actions taken throughout the federal government to identify additional travel automation opportunities and processing efficiencies for the Board.
- Although the Board's initiative in 2004 to replace its automated travel system did not result in a new system acquisition, the Board did adopt a more formal project management process as part of that effort, including establishing project teams with Boardwide representation, developing mandatory and desirable system requirements based on division input, and conducting Boardwide user testing. These efforts are responsive to the first two recommendations in our 2004 report.
- With the recent adoption of SATO Travel and the new reservation process, MGT staff provided a "Quick Tips" guide for staff's use and a help desk is also available. In addition, MGT has been working to improve travel processing by tracking the number of adjustments made to expense statements and providing feedback to help teach travelers and reviewers. These actions are responsive to the third recommendation in our 2004 report.

Inspections and Evaluations

The Inspections and Evaluations program area encompasses OIG inspections, program evaluations, enterprise risk management activities, process design and life-cycle evaluations, and legislatively-mandated material loss reviews of failed financial institutions that the Board supervises. Inspections are generally narrowly focused on a particular issue or topic, and provide time-critical analysis that cuts across functions and organizations. In contrast, evaluations are generally focused on a specific program or function, and make heavy use of statistical and quantitative analytical techniques. Evaluations can also encompass other non-audit, preventive activities such as System Development Life Cycle projects, and participation on task forces and workgroups. With the exception of the follow-up highlighted below, our work in this program area is ongoing and will be reported during the next semiannual period.

Follow-up of the Review of the Fine Arts Program

During this reporting period, we completed a follow-up of our April 2004, *Review of the Fine Arts Program*. The report contained two recommendations designed to strengthen the Fine Arts Program's (Program) financial, inventory, and managerial internal controls. Our first recommendation, addressed to the Committee on Board Affairs (CBA), was to reexamine the appropriateness of the Program's practice of soliciting cash and works of art donations. Our follow-up work found that the CBA determined that the Board has adequate controls to prevent obtaining donations from prohibited sources. The CBA also confirmed that soliciting tax deductible gifts from individuals and philanthropic organizations is an appropriate means to acquire works of art and expand the Board's collection.

Our second recommendation was addressed to the director of MGT and focused on strengthening the Program's internal controls and improving overall Program operations. More specifically, this multi-part recommendation called for establishing written policies and procedures for receiving works of art through existing Board processes; implementing a single fine arts inventory management system; instituting annual physical inventory counts of the fine arts collection; and ensuring that donated works of art are valued by an independent appraiser. The director of MGT and the CBA generally agreed with our recommendation; however, they decided that an independent appraisal on work of art would not be cost effective given the Board's position on insurance and resale. We have determined that actions taken are sufficient and we have closed both recommendations.

Investigations

The OIG's Investigations program conducts criminal and administrative investigations relating to the Board's programs and operations. To effectively carry out its mission, OIG special agents must possess a thorough knowledge of current federal criminal statutes and the rules for criminal procedure, as well as other rules, regulations, and court decisions governing the conduct of criminal, civil, and administrative investigations. OIG special agents have full law enforcement authority as a result of a blanket deputation agreement with the Department of Justice (U.S. Marshals Service). As Special Deputy Marshals, OIG agents are authorized to carry firearms, and to obtain and execute search and arrest warrants, as necessary.

As the challenges to the federal law enforcement community have increased in the post 9-11 era, so have the challenges to the financial regulators to implement new requirements for banks to detect illegal activities, such as money laundering and terrorist financing. As a result, the nature and complexity of our investigations have also increased the challenges to our special agents. During this reporting period, our criminal investigative activity involved leading or participating in multi-agency task forces where bank fraud, terrorist financing, and money laundering were often the potential crimes being investigated.

In addition, our special agents 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. The following are highlights of investigative cases closed during the past six months:

- **Employee Misconduct:** In February 2006, the OIG initiated an investigation after receiving an allegation that a Board employee provided an unauthorized Board memorandum to a prospective mortgage lender, as verification of income and future grade and salary increases. The investigation disclosed that the Board employee sent the memorandum from a fax machine located near the employee's office to a loan officer at the mortgage company. In addition, a computer forensic examination of the employee's computer disclosed three partial e-mail messages revealing a personal relationship between the employee and the loan officer. The investigation also revealed that the document was transmitted to the mortgage company more than three hours after the employee's supervisor had indicated that he could not sign the letter. While the employee acknowledged preparing and sending the letter to the broker, the employee denied signing the supervisor's name to the document. The investigation did not disclose the identity of the person who signed the verification letter. Based on the results of our investigation, the employee resigned in lieu of termination.
- **Illegal Drug Use by a Federal Reserve Board Law Enforcement Officer:** In July 2006, the Assistant Chief of the Board's Law Enforcement Unit (LEU) requested that the OIG initiate an investigation into allegations that

an unidentified female officer of the LEU reportedly asked contract employees to provide her with a sample of their urine for her drug test. The officer was suspected to be one of three officers selected for drug screening that day. Subsequent investigation by the OIG revealed the officer's identity. During an interview with OIG special agents, the officer confessed to illegal drug use and subsequently resigned in lieu of facing potential administrative action, up to and including termination of employment.

- Alleged Workers' Compensation Fraud:** During the course of an OIG evaluation of the Board's administration of the Office of Workers' Compensation Program, a number of fraud indicators were identified in conjunction with former employees' receipt of permanent long-term disability. The evaluation team referred these indicators to Investigations for further review. Our special agents completed three separate investigations of potential workers' compensation fraud by former Board employees. The investigations did not disclose any evidence of fraudulent activity by the former employees, and we referred the results of our investigations to the Board's Legal Division for appropriate action.

Summary Statistics on Investigations for the Period April 1 through September 30, 2006

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	4
Investigations Open from Previous Period	15
Investigations Closed during Reporting Period	8
Total Investigations Active at End of Reporting Period	11
Investigative Results for this Period	
Referred to Prosecutor	2
Joint Investigations	8
Referred for Audit	0
Referred for Administrative Action	1
Oral and/or Written Reprimand	0
Terminations of Employment	2
Arrests	0
Suspensions	0
Debarments	0
Indictments	0
Convictions	0
Monetary Recoveries	\$0
Civil Actions (Fines and Restitution)	\$0
Criminal Fines: Fines & Restitution	\$0

Hotline Operations

Our investigators continue to review all complaints received from the toll-free Hotline number, correspondence, email and facsimile communications, requests from Federal Reserve System employees, and members of the public. The information received is analyzed to determine if further inquiry is warranted and provides the basis for potential investigations. Most hotline contacts were calls

from 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 OIG's, and other financial regulatory agencies. We directed those inquiries to the appropriate Board offices, Reserve Banks, or federal or state agencies.

In addition, we continually receive 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 following table:

Summary Statistics on Hotline Results for the Period of April 1 through September 30, 2006

Hotline Complaints	Number
Complaints pending from the previous reporting period	2
Complaints received during this reporting period	143
Total complaints for the Reporting Period	145
Complaints resolved during this period	122
Complaints pending	23

Legal Services

The Legal Services Program furnishes the OIG with comprehensive legal services (including legal advice, formal written opinions, counseling, and representation, based upon extensive research and critical analysis of relevant laws, regulations, and policies) to support its professional and administrative functions. This work often provides the legal basis for conclusions, findings, and recommendations in various OIG reports. The Legal Services staff also keeps the IG and OIG staff aware of recent developments in the law that may have an impact on the activities of the OIG and the Board. Additionally, Legal Services handles Freedom of Information Act (FOIA) and Privacy Act requests, and reviews and prepares administrative subpoenas. Legal Services staff also participate regularly in professional and IG community activities relating to the OIG's mission. During this reporting period, Legal Services provided continuing professional education to OIG staff on Regulations P and Z, and the Computer Matching Act.

Pursuant to the IG Act, as amended, we regularly track and review existing and proposed legislative and regulatory items that have potential impact on the activities of the Board, including the OIG. Legal Services staff conduct independent analyses of new or proposed legislation and regulations to determine their effect on the efficiency or effectiveness of the programs and operations of the Board. During this reporting period, we reviewed thirty-five legislative items. The following table highlights our work in this area.

Highlights of the OIG's Review of Laws and Regulations, April 1 through September 30, 2006

Legislation Reviewed	Purpose/Highlights
Board/Banking-related Legislation	
Unlawful Internet Gambling Enforcement Act (H.R. 4411) [became Title VIII of Public Law 109-347]	Prevents the use of certain payment instruments, credit cards and fund transfers for unlawful internet gambling. Requires the Board to prescribe regulations, policies, and procedures to identify and block prohibited transactions.
Seasoned Customer CTR Exemption Act of 2006 (H.R. 5341)	Exempts depository institutions from having to file currency transaction reports (CTRs) for qualified customers.
Competitive and Open Markets that Protect and Enhance the Treatment of Entrepreneurs Act (H.R. 5405)	Reduces the burden of implementation of section 404 of the Sarbanes-Oxley Act of 2002 by exempting small companies from having to file internal control reports.
Financial Services Regulator Relief Act of 2006 (S. 2856) [became Public Law 109-351]	Provides regulatory relief and improves productivity for insured depository institutions, and for other purposes.
House Resolution 909	Encourages the financial services industry to prepare for pandemics and bio terrorism.

Highlights of the OIG's Review of Laws and Regulations, April 1 through September 30, 2006 (continued)

Legislation Reviewed	Purpose/Highlights
Inspector General/Law Enforcement-related Legislation	
Government Credit Card Abuse Prevention Act of 2006 (H.R. 5581)	A bill to prevent abuse of government credit cards. Requires OIG's to conduct risk assessments and audits to detect fraud, and to report findings to the head of the agency, OMB, and the Comptroller General.
National Capital Transportation Amendments Act of 2006 (H.R. 3496)	Among other things, creates an OIG for the Washington Metropolitan Area Transit Authority.
Judicial Transparency and Ethics Enhancement Act of 2006 (H.R. 5219 & S. 2678)	A bill to establish an OIG for the Judicial Branch.
Intelligence Authorization Act for Fiscal Year 2007 (S. 3237)	A bill to establish an OIG for the Intelligence Community within the Office of the Director of National Intelligence.
National Transportation Safety Board (NTSB) Reauthorization Act of 2006 (S. 3679)	Among other things, designates the Department of Transportation IG as Inspector General of the NTSB.
Information & Data Security/Privacy-related Legislation	
Federal Agency and Data Privacy Protection Act (H.R. 5820); Veterans Identity and Credit Security Act of 2006 (H.R. 5835); Financial Data Protection Act(s) of 2005 / 2006 (H.R. 3997 / S. 2169); Data Accountability and Trust Act (H.R. 4127); Notification of Risk to Personal Data Act (H.R. 5582); Data Theft Protection Act of 2006 (S. 3506 & H.R. 5661); Federal Agency Data Breach Notification Act (H.R. 5838)	Various bills to enhance the security and privacy associated with the government's handling of personal and financial information. Proposed means include, among others, establishment of encryption requirements, data breach notification policies and standards, restrictions on physical removal of information held by government agencies, imposition of security measures on credit reporting agencies and information brokers.
Open Government Act of 2005 (H.R. 867 & S. 394)	Amends the FOIA by holding agencies more strictly accountable, and relaxes certain requester requirements.
Federal Agency Protection Privacy Act of 2005 (H.R. 2840)	Requires federal agencies to conduct privacy impact assessments for proposed rulemakings.

Community Participation and Internal Operations

While the OIG's primary mission is to enhance Board programs and operations, we also coordinate externally and work internally to achieve our goals and objectives. Externally, we are active members of broader IG and professional communities and promote coordination on shared concerns. Internally, we continue to leverage information technology (IT) to enhance and streamline business processes and to ensure the security of our information resources. Highlights of our activities follow:

Executive Council on Integrity and Efficiency (ECIE) Participation

The Board's IG serves as the Vice Chair of the ECIE, which was created by Executive Order in 1992 to facilitate coordination among IGs of designated Federal entities. As Vice Chair, the Board's IG provides leadership, vision, and direction to the ECIE, and represents the ECIE on the President's Council on Integrity and Efficiency (PCIE). He promotes professionalism and coordination among the Councils' membership, provides a forum to discuss government-wide issues and shared concerns, and facilitates work on a wide range of Council projects and initiatives. Collectively, the members of the ECIE continue to work with the members of the PCIE on a number of issues to help improve Government programs and operations.

Advisory Council on Government Auditing Standards

To help ensure that *Government Auditing Standards* (the "Yellow Book") continue to meet the needs of the audit community and the public it serves, the Comptroller General of the United States appointed the Advisory Council on Government Auditing Standards to review the standards and recommend necessary changes. The Council includes experts in financial and performance auditing drawn from all levels of government, private enterprise, public accounting, and academia. The Board's IG participates as a member of the Advisory Council and provides perspective on a variety of issues and proposals related to the standards.

IT Infrastructure Enhancements

During this reporting period, the OIG made substantial progress in upgrading and enhancing its IT infrastructure to more efficiently and effectively support the audit, evaluation, investigative, and legal work discussed in the earlier sections of our report. Consistent with our IT strategy, we completed an upgrade of our servers, ensuring a more reliable and responsive environment. We also created a central database to consolidate, organize, and document our IT infrastructure to help ensure OIG compliance with FISMA.

Chairman and New Governor Orientation

During this reporting period, the Board's Chairman and two new Governors visited the OIG to meet our staff and to learn more about the mission, organization, and responsibilities of our office and the IG community. These orientation sessions provided an excellent opportunity to share information about our work and the unique role that IGs play in conducting independent and objective audits, investigations, inspections, and evaluations of agency programs and operations.

Appendixes

Appendix 1
Audit Reports Issued with Questioned Costs for the Period April 1 through
September 30, 2006

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	0	\$0	\$0
For which a management decision was made during the reporting period	0	\$0	\$0
(i) dollar value of disallowed costs	0	\$0	\$0
(ii) dollar value of costs not disallowed	0	\$0	\$0
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 April 1 through September 30, 2006

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	09/06	9	0
Audit of the Federal Reserve's Background Investigation Process	10/01	3	3	0	04/04	0	3
Audit of Retirement Plan Administration	07/03	4	3	1	06/05	3	1
Audit of the Board's Outsourcing Operations	04/04	3	3	0	-	-	-
Review of the Fine Arts Program	04/04	2	2	0	05/06	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	09/06	3	2
Audit of the Board's Automated Travel System	11/04	4	4	0	09/06	4	0
Review of the Board's Workers' Compensation Program	03/05	4	4	0	-	-	-
Review of the Board's Implementation of Software Security Reviews	05/05	1	0	1	-	-	-
Audit of the Board's Fixed Asset Management Process	05/05	2	2	0	03/06	1	1
Evaluation of Service Credit Computations	08/05	3	3	0	-	-	-
Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act	09/05	4	3	1	09/06	2	2
Audit of the Board's Information Security Program	10/05	2	2	0	09/06	0	2
Inspection of the Board's Security Services Unit	03/06	3	3	0	-	-	-
Audit of the Board's Implementation of Electronic Authentication Requirements	03/06	1	1	0	09/06	0	1
Audit of the Board's Information Security Program	09/06	2	2	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	12-13
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 prosecutorial authorities	10
5(a)(5)/6(b)(2)	Summary of instances where information was refused	None
5(a)(6)	List of audit reports	4-6
5(a)(7)	Summary of significant reports	None
5(a)(8)	Statistical Table—Questioned Costs	19
5(a)(9)	Statistical Table—Recommendations that Funds Be Put to Better Use	20
5(a)(10)	Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made	19-20
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*

