



Office of Inspector General Semiannual Report to Congress

October 1, 2005 – March 31, 2006





Semiannual Report to Congress

October 1, 2005 – March 31, 2006

OIG

Office of Inspector General



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

OFFICE OF INSPECTOR GENERAL

April 27, 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 October 1, 2005, through March 31, 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

October 1, 2005 – March 31, 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	10
Legal Services.....	13
Community Participation and Internal Operations	16
Appendixes	17
Appendix 1—Audit Reports Issued with Questioned Costs for the Period October 1, 2005, through March 31, 2006	19
Appendix 2—Audit Reports Issued with Recommendations that Funds be Put to Better Use for the Period October 1, 2005, through March 31, 2006.....	20
Appendix 3—OIG Reports with Outstanding Recommendations.....	21
Appendix 4—Cross-References to the Inspector General Act	22

Introduction

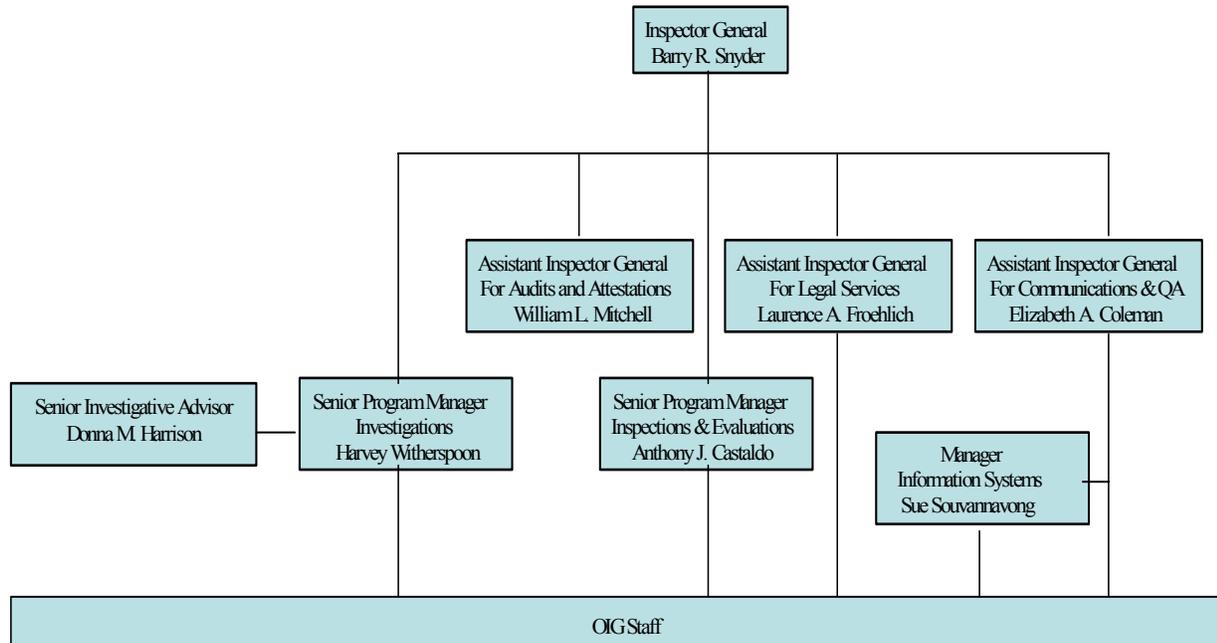
Consistent with the Inspector General Act of 1978 (IG Act), as amended, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- 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 that include evaluating the effectiveness of security controls and techniques for selected information systems.

OFFICE OF INSPECTOR GENERAL

February 2006

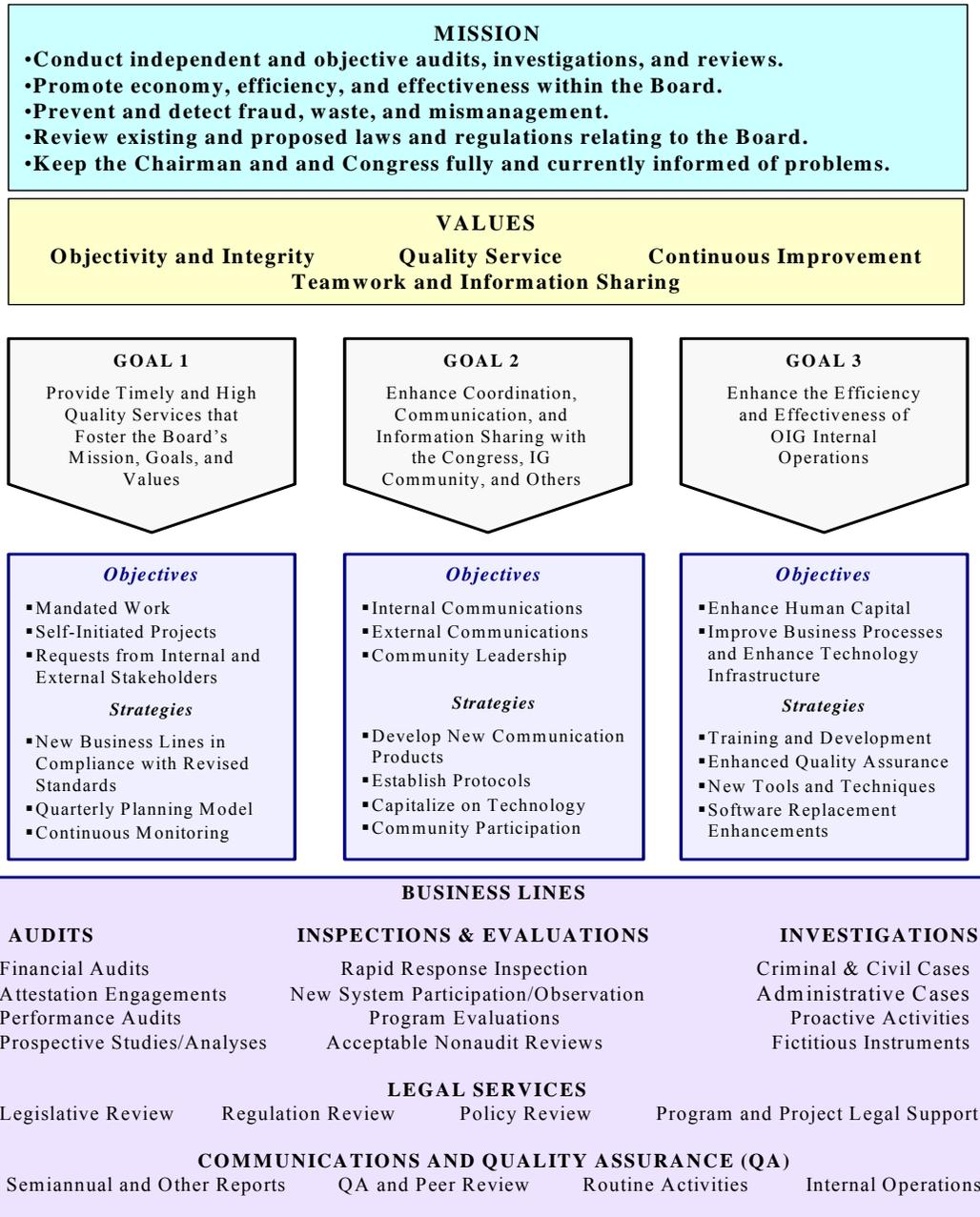


OIG Staffing	
Auditors	17
EDP Auditors	7
Investigators	5
Attorneys.....	2
Administrative.....	2
Information Systems Analysts.....	3
Total Authorized Positions	36

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 the economy and 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, including controls used in computer-based systems; 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, as well as our follow-up activities.

Report on the Audit of the Board's Implementation of Electronic Authentication Requirements

On December 17, 2002, the E-Government Act of 2002, Public Law 107-347 (E-Gov Act) was enacted to, among other things, enhance citizen access to government information and services and to improve government operations, primarily through expanded use of the Internet. The E-Gov Act requires each agency to ensure that the methods it uses to secure access to electronic government information and services are in accordance with relevant policies and procedures issued by the Director of the Office of Management and Budget (OMB) and applicable technical guidance developed by the National Institute of Standards and Technology (NIST). We began this audit as part of an effort to perform work throughout the year related to our independent evaluation responsibilities under FISMA. The objectives of our audit were to (1) determine whether the Board appropriately identified the systems requiring e-authentication assessments, (2) determine whether the Board prepared assessments in accordance with guidance issued by OMB and NIST, and (3) evaluate how e-authentication requirements are being included in the Board's revised information security program.

We found that the Board identified and completed e-authentication risk assessments for seven applications that provide access to remote users. However, we identified at least two additional applications accessed by other government agencies and third parties outside the Federal Reserve System for which e-authentication risk assessments were not completed. In addition, we found that the risk assessments prepared for the seven applications were not completed consistently across divisions and that five of these assessments had variations from OMB guidance. Because the Board's information security program was in a period of transition at the time the assessments were completed, the Information Security Officer (ISO) had not developed specific e-authentication guidance, and related guidance (such as procedures for risk assessments and certification and accreditation) had not been finalized. The seven e-authentication assessments were completed primarily to fulfill a specific OMB annual reporting requirement,

as opposed to being an integral part of a broader information security lifecycle framework.

During our audit fieldwork, we shared our initial observations with the Board's information security staff, and the ISO incorporated our input into a revised risk assessment guide, which includes specific e-authentication guidance. The draft guidance addresses many of the issues identified during the audit and provides additional information to assist system owners in completing the e-authentication risk assessments once the requirement for an assessment has been determined. The e-authentication risk assessments will now be part of the overall risk assessment process which should help ensure that all systems meeting the e-authentication requirements have been identified. Our report contains a recommendation for the Chief Information Officer (CIO) to finalize the e-authentication guidance, including processes for validating and periodically reassessing assurance levels, and to ensure that all applications meeting e-authentication requirements are identified and properly assessed. The CIO concurred with our recommendation and identified several actions underway or completed to strengthen the Board's e-authentication process.

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 contracted 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.

During the reporting period, the auditors completed fieldwork related to the FFIEC audit and issued the audit report. In the auditors' opinion, the FFIEC's financial statements present fairly, in all material respects, the FFIEC's financial position 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 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 FFIEC'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*.

The auditors are continuing fieldwork on the Board's financial statements and the results will be included in our next semiannual report.

National Science Foundation OIG Peer Review

We reviewed the system of quality control for the audit function of the National Science Foundation (NSF) OIG in effect for the year ended September 30, 2005. A system of quality control encompasses an OIG's organizational structure, and the policies adopted and procedures established to provide it with reasonable assurance of conforming with generally accepted government auditing standards (GAGAS). GAGAS requires government audit organizations to undergo periodic external peer reviews, in order to determine whether the OIG's internal quality control system is adequate as designed and complied with to provide reasonable assurance that applicable auditing standards, policies, and procedures have been met. Our review was conducted in conformity with standards and guidelines established by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE); a final report was provided to the NSF Inspector General.

Follow-up of the Audit of the Board's Efforts to Implement Performance Management Principles Consistent with the Results Act

During the reporting period, we completed a second follow-up related to our July 2001 *Report on the Board's Efforts to Implement Performance Management Principles Consistent with the Results Act*. That report contained four recommendations to enhance the Board's planning and budgeting process. Our initial follow-up, completed in 2003, determined that the Board was current with the Government Performance Results Act of 1993 (GPRA) reporting requirements, as a result of issuing an updated strategic planning document, biennial performance plan, and performance report. However, we recognized that the planning and budgeting process for 2004-2005 was the first opportunity for the Board to fully implement the report's recommendations. As a result, we decided to keep the recommendations open.

During our second follow-up, we met with Board management and staff, and also reviewed pertinent documents. We found that the Board has developed a

framework of encouraging results-oriented performance management and has revised its strategic planning process to focus on the Board's mission, goals, and objectives and to better integrate overarching issues. We also found that management has revised performance measures that are aligned from the strategic plan to the performance objectives and expectations of division officers. In addition, the Board issued a GPRA performance report which includes a comparison of actual program results with established performance goals and measures. We believe these actions are sufficient to close the four recommendations.

Follow-up of the Audit of the Board's Fixed Asset Management Process

Our May 2005 audit report contained two recommendations designed to address fixed asset management issues related to policies, financial system usage, and internal controls. Our first recommendation was for the Board to develop an overall property management policy that specified the requirements and responsibilities for the receipt, tracking, and disposal of Board assets, including requirements for conducting periodic physical inventories. The recommendation also addressed the need to finalize the related accounting policies and procedures to ensure consistency with the revised policy. Our follow-up work found that the Board issued a new property management policy which incorporates accounting-related policies and procedures; we, therefore, closed this recommendation. Our second recommendation was to strengthen internal controls over the Board's property management process by fully implementing available functionality in the Board's financial system, ensuring that sufficient descriptive information is recorded for each asset, and improving controls over the disposal process. Staff in the Board's Management Division (MGT) told us that additional financial system functionality will be implemented and the property management process will include the use of a new form to facilitate the recording of capital assets in the Board's financial system. Our follow-up work also found that MGT established a separation of duties between the property manager and the accounting function. In approximately six months, we plan to perform limited testing of assets purchased subsequent to the issuance of the new policy and the implementation of revised asset management procedures. Once this follow-up work is completed, we anticipate closing the second recommendation.

Inspections and Evaluations

The Inspection and Evaluation 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. Highlights of our work in this area follow.

Report on the Inspection of the Board's Security Services Unit

During this period, we completed an inspection of the Board's Security Services Unit (SSU). The USA PATRIOT Act of 2001 granted the Board certain federal law enforcement authorities, and the regulations implementing this new authority—Uniform Regulations for Federal Reserve Law Enforcement Officers (Uniform Regulations)—designated the Board's OIG as the External Oversight Function (EOF). We performed this inspection to fulfill our EOF responsibility to review and evaluate the Board's law enforcement programs and operations.

The objective of this inspection was to provide reasonable assurance that the Board's SSU was in compliance with the Uniform Regulations, Board and SSU internal policies and procedures, and where applicable, law enforcement best practices. To accomplish this objective, we developed an instrument to guide our inspection data collection, observation, and testing activities. Our approach was based on an analysis of the USA PATRIOT Act of 2001; the Board's Uniform Regulations; the General Policies And Procedures for the Board's Law Enforcement Officers; the SSU's Manual of General Orders; the Federal Law Enforcement Training Accreditation Standards Manual; the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*; and the SSU Internal Oversight Committee report.

As part of our inspection activities, we performed a comprehensive firearms inventory, and conducted a compliance inspection of training and personnel files for a randomly-selected sample of fifteen Federal Reserve Law Enforcement Officers. In addition, we interviewed Board and SSU management and staff, and law enforcement training officials at the Departments of Energy and State, and the Federal Law Enforcement Training Accreditation's Office of Accreditation. We conducted our work in accordance with the *Quality Standards for Inspections* issued by the PCIE and ECIE.

During the course of the inspection, nothing came to our attention to indicate material non-compliance with the Board or SSU policies and procedures, or

substantive deficiencies in SSU's internal control environment. However, the inspection report included three recommendations designed to enhance SSU's operations and internal controls. We presented the inspection results to the Director of the Management Division who concurred with each recommendation. Our report will not be made available to the public because it contains security-related information.

Follow-up of the Evaluation of Key Emergency Preparedness and Security Enhancements

Our 2004 report, which was not released to the public because it addressed sensitive security-related information, contained four recommendations. Our follow-up work included discussions with Board officials and staff, and a review of pertinent documents, policies, procedures, and practices. We closed each of the four recommendations after determining that sufficient actions have been taken, or are in process.

Investigations

Investigative Activity

The OIG's Investigative Services program conducts criminal and administrative investigations related to the Board's programs and operations. All OIG agents are fully trained and 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.

Since September 11, 2001, the nature of our workload has evolved. As the challenges to the federal law enforcement community have increased, our experience and expertise in the financial regulatory environment have been especially in demand. Growth in the number and complexity of investigations continue to present new challenges to our staff of investigators. Much of our criminal investigation activity now involves leading or participating in multi-agency task forces where bank fraud, terrorist financing, and money laundering are often the potential crimes being investigated.

The following are highlights of our significant investigative activity over the last six months:

- **Alleged Prime Bank Fraud:** On November 2, 2005, the OIG received a request from the U. S. Secret Service for assistance with a criminal investigation regarding a prime bank fraud case involving a private hedge fund company and a board member of a Federal Reserve-regulated institution. The fraud was perpetrated by using the Federal Reserve's name and claiming that the investments were overseen by a "Federal Reserve Administrator." On November 12, 2005, the now-former director, and two associates, were arrested and charged with wire fraud. The complaint filed by the U.S. Attorney's Office alleged that the three men made false statements to the hedge fund manager so that they could keep the \$25 million invested with a Nevada-based company. We are continuing to work jointly with the U.S. Secret Service and the Assistant United States Attorney.
- **Conspiracy to Violate U.S. Immigration Laws:** In February 2006, Immigration and Customs Enforcement (ICE) contacted OIG Special Agents to request assistance with an investigation of numerous individuals involved in a conspiracy to violate U.S. immigration laws, and which involved a Federal Law Enforcement Officer at a Federal Reserve Bank. In conjunction with ICE's execution of multiple search and arrest warrants, OIG agents interviewed and obtained a written statement from the employee in question. Following certain admissions, the employee was placed on administrative leave and subsequently terminated from his position. We are continuing to work jointly with ICE on this matter and are awaiting a decision by the Assistant United States Attorney regarding potential criminal charges against the former employee.

- **Employee Misconduct:** In October 2005, the Board’s Chief of Security Services requested that the OIG initiate an investigation of a uniformed training officer for misconduct related to the employee’s failure to notify his superiors regarding multiple citations issued by the Maryland State Police. Based on the results of our investigation and a subsequent arrest of the employee on other charges, the employee has resigned in lieu of termination.
- **National Labor Relations Board OIG Peer Review:** We conducted an external quality assessment review of the National Labor Relations Board (NLRB) OIG’s investigative function in effect for the period ended October 2005. The objective of this qualitative assessment review was to determine whether NLRB OIG’s internal safeguards and management procedures were in place and operating effectively to provide reasonable assurance that established policies, procedures, and applicable investigative standards were met. Our review was conducted in conformity with applicable quality standards for OIG investigations and related review guidelines, and a final report was provided to the NLRB Inspector General.

Summary Statistics on Investigations for the Period October 1, 2005, through March 31, 2006

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	7
Investigations Open from Previous Period	8
Investigations Closed during Reporting Period	0
Total Investigations Active at End of Reporting Period	15
Investigative Results for this Period	
Referred to Prosecutor	2
Joint Investigations	7
Referred for Audit	0
Referred for Administrative Action	1
Oral and/or Written Reprimand	0
Terminations of Employment	2
Arrests	3
Suspensions	0
Debarments	0
Indictments	1
Convictions	0
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. These complaints are received from our 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. Most hotline contacts were calls from consumers with complaints or questions about practices of private financial institutions involving 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.

In addition, we continue to 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 October 1, 2005, through March 31, 2006

Complaints Referred for Investigation	Number
From the previous reporting period	9
During this reporting period	88
Total for Reporting Period	97
Complaints resolved during this period	95
Complaints pending	2

Legal Services

During this reporting period, the Legal Services program contributed to OIG audits, investigations, inspections, and other operations by providing legal advice and support in all areas of the OIG’s activities. This work was based on extensive legal research and critical analysis of laws, legislation, regulations and policies that relate to, or have an impact on, the OIG’s work. Legal Services staff also handle incoming Freedom of Information Act (FOIA) requests, and review and prepare subpoenas for issuance by the Inspector General. In addition, Legal Services regularly participates in professional activities that support or relate to the OIG’s mission, and is actively involved in IG legal issues on a community-wide basis. The following table provides selected highlights of Legal Services staff’s work.

Legal Advice and Counseling	Information Handling	Professional and Community Activities
<ul style="list-style-type: none"> • E-authentication and FISMA issues • Inspection of the Board’s SSU • Audit of the Board’s Payroll Processes • Interpretations of contract provisions of Board’s Financial Statement Audit • Law enforcement deputation for OIG criminal investigators 	<ul style="list-style-type: none"> • FOIA requests • Issuance of IG subpoenas • Training for OIG staff on handling grand jury information • OIG Privacy Act Systems Notice Revisions 	<ul style="list-style-type: none"> • Council of Counsels to the IGs • George Washington University Law School Government and Public Interest Internship Program • IG Counsels’ Working Group on Legal Aspects of Investigative Best Practices

The Legal Services program area also keeps the Inspector General and OIG staff aware of recent developments in the law through our legislative and regulatory review process, and the review and analysis of executive orders, government-wide policies, guidance, and other legal materials. Pursuant to the IG Act, we review existing and proposed legislative and regulatory items; we routinely track proposed and pending legislation and regulations and independently analyze the effect that the new or proposed legislation, regulation, or policy may have on the efficiency and effectiveness of the programs and operations of the Board, including the OIG. The following table highlights our work in this area during the current reporting period.

Highlights of the OIG's Review of Laws and Regulations, October 1, 2005, through March 31, 2006

Legislation Reviewed	Purpose/Highlights
Board/Banking-related Legislation	
Presidential \$1 Coin Act of 2005 (S. 1047—became Pub.L. 109-145)	Among other things, requires that \$1 coins be minted in commemoration of the nation's past Presidents, and requires the Board and the Secretary of Treasury to ensure adequate circulation of \$1 and other coins.
National Defense Authorization Act for Fiscal Year 2006 (H.R. 1815—became Pub.L. 109-163)	Section 579 requires the Secretary of Defense, after consultation with the Chairman of the Federal Reserve, to provide a report to Congress regarding predatory lending against Armed Service members.
Hurricane Check Cashing Relief Act of 2005 (H.R. 3909)	A bill to provide authority to the Federal Deposit Insurance Corporation and the National Credit Union Administration, in accordance with guidance issued by the Board to guarantee checks cashed for the benefit of non-customers who are victims of the 2005 hurricanes, and for other purposes.
Consumer Checking Fairness Act (H.R. 4415)	To establish a fair order of posting checks and deposits in order to prevent unjust enrichment of financial institutions, and for other purposes.
Liberty Bill Act (S. 2056)	A bill to redesign the \$1 Federal Reserve Note.
Inspector General/Law Enforcement-related Legislation	
Combating Money Laundering & Terrorist Financing Act of 2006 (S. 2402)	To improve prohibitions on money laundering, and for other purposes.
Foreign Agents Compulsory Ethics in Trade Act of 2006 (H.R. 4690)	To amend section 207 of title 18, United States Code, to further restrict Federal officers and employees from representing or advising foreign entities after leaving Government service.
Intelligence Authorization Act for Fiscal Year 2006 (S. 1803)	Among other things, repeals section 8K of the Inspector General Act, and amends the National Security Act to establish an Inspector General for the Intelligence Community.
Data Information/Privacy-related Legislation	
Financial Data Security Act of 2005 (H.R. 3375)	Amends the Fair Credit Reporting Act by placing requirements on Credit Reporting Agencies to protect and secure sensitive identifiable financial information. Also imposes rulemaking requirements on the Board.
Consumer Notification and Financial Data Privacy Act of 2005 (H.R. 3374)	Imposes data security requirements on financial institutions. Includes enforcement provisions to be enforced, in certain cases, by the Board.
Personal Data Privacy and Security Act of 2005 (S. 1332 & S. 1789)	A bill to prevent and mitigate identity theft.

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 strengthen our investment in our human capital with a new e-learning initiative and to leverage technology to enhance and streamline business processes. Highlights of our activities follow.

Executive Council on Integrity and Efficiency Participation

The Board's Inspector General (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 on behalf of the Council Chair (Deputy Director for Management, Office of Management and Budget). 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.

IG E-Learning Initiative

The OIG actively participates in a PCIE/ECIE pilot program that offers additional learning opportunities to IG employees. Launched in July 2005, the Inspector General's E-Learning (IGEL) initiative offers numerous on-line courses tailored to meet the training needs of auditors, investigators, administrative and legal staff. IGEL's extensive, on-line library is a valuable reference tool that has proven

useful when planning audits and researching current and relevant information for use during on-going assignments.

Our office has enthusiastically embraced this initiative. Sixty-five percent of our employees have either completed courses to gain new skills and to maintain their competency, or have used the on-line search feature to identify information relevant to on-going assignments.

IT Infrastructure Enhancements

During this reporting period, the OIG began an effort to upgrade and enhance our IT infrastructure to more efficiently and effectively support the audit, evaluation, legal, and investigative work discussed in the earlier sections of our report. We migrated our IT environment to a new operating system and made corresponding upgrades in other key software. Consistent with our IT strategy, we also replaced laptops and are in the process of upgrading dated servers to ensure a more reliable and responsive environment. We anticipate completing the rollout during the next reporting period.

Appendixes

Appendix 1

Audit Reports Issued with Questioned Costs for the Period October 1, 2005, through March 31, 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 October 1, 2005, through March 31, 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	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	03/06	4	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	–	–	–
Evaluation of Key Emergency Preparedness and Security Enhancements	05/04	4	4	0	01/06	4	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	09/05	2	3
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	–	–	–
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	–	–	–
Audit of the Board's Information Security Program	10/05	2	2	0	–	–	–
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	–	–	–

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	14
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	4-7
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	21
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*

