

Office of Inspector General
Semiannual Report to Congress

April 1 – September 30, 2007



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

OFFICE OF INSPECTOR GENERAL

October 31, 2007

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, 2007. 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/

Elizabeth A. Coleman
Inspector General

Enclosure



Semiannual Report to Congress

April 1 – September 30, 2007

OIG

Office of Inspector General

Table of Contents

	Page
Introduction.....	1
Goals and Objectives	3
Audits and Attestations.....	4
Inspections and Evaluations.....	9
Investigations	14
Legal Services.....	17
Community Participation and Internal Operations	21
Appendixes	23
Appendix 1—Audit Reports Issued with Questioned Costs for the Period April 1 through September 30, 2007	25
Appendix 2—Audit Reports Issued with Recommendations that Funds be Put to Better Use for the Period April 1 through September 30, 2007.....	26
Appendix 3—OIG Reports with Outstanding Recommendations.....	27
Appendix 4—Cross-References to the Inspector General Act	28

Introduction

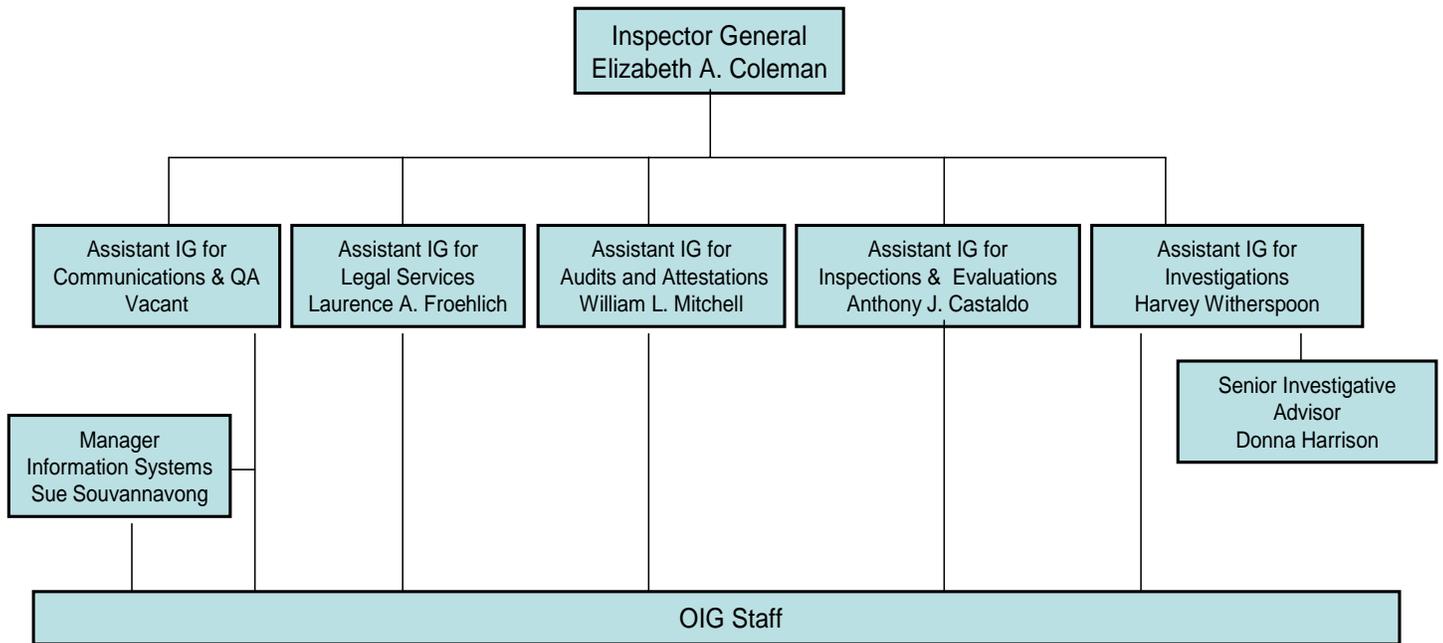
Consistent with the Inspector General Act of 1978 (IG Act), as amended, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- 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 influence 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 fund, 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 2007

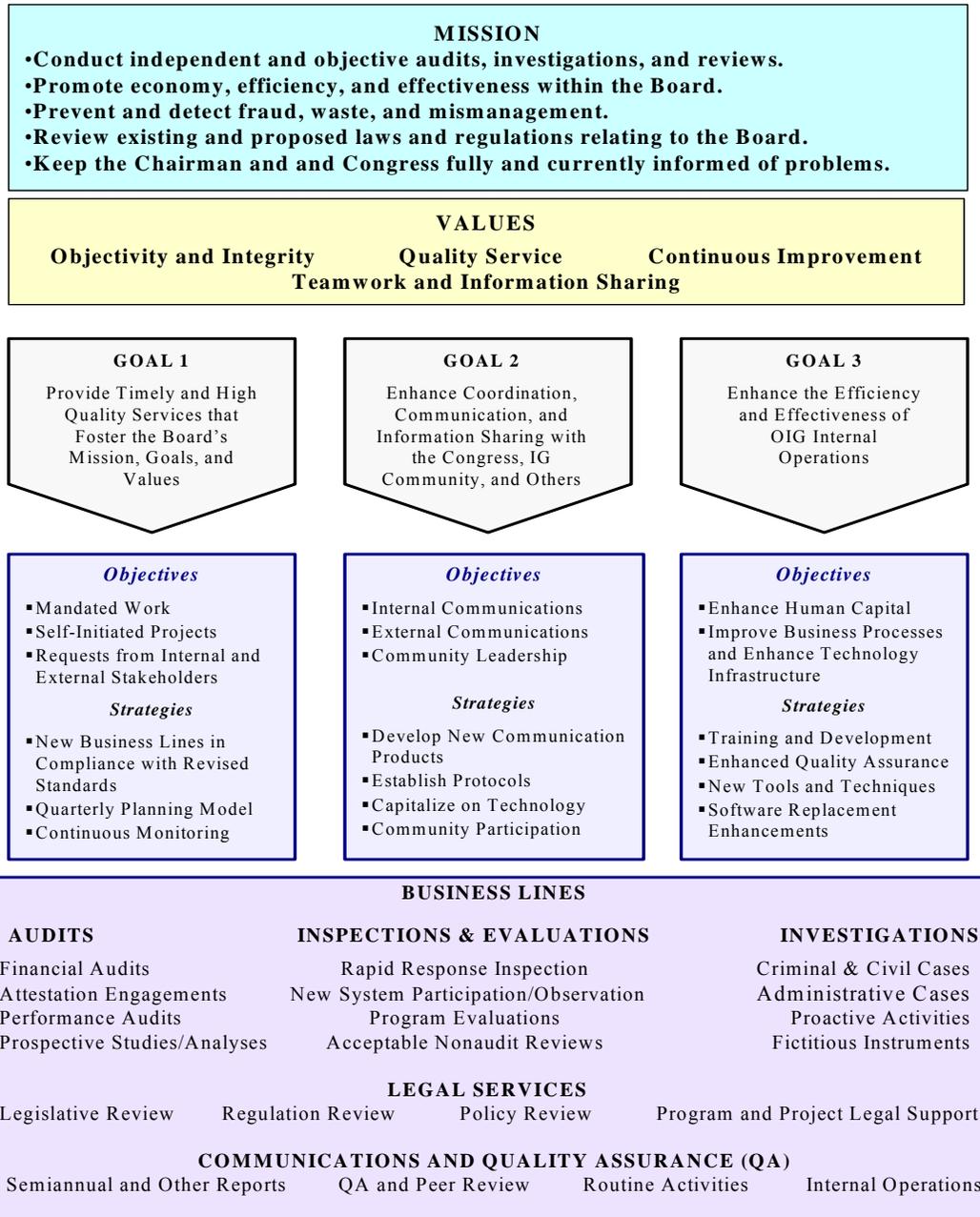


OIG Staffing	
Auditors	18
Information Technology Auditors	6
Investigators	5
Attorneys.....	2
Administrative.....	2
Information Systems Analysts.....	3
Total Authorized Positions	36

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 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 OIG work completed during the reporting period, including our follow-up activities, as well as work that will continue into the next semiannual reporting period.

Audit of the Board's Information Security Program

During the reporting period, we completed an audit of the Board's information security program and practices. This audit was performed pursuant to FISMA which requires 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 Act'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 three Board applications and followed up on the open issues from our 2006 application control reviews. We also recently began a review of controls provided by the Federal Reserve Bank of Boston for applications that the Reserve Bank maintains in support of the Board's supervision and regulation function. We performed our 2007 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*. These control tests identified areas where security 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.” Given the sensitivity of the issues involved with these reviews, we will provide the specific results to management in separate restricted reports. In addition, follow-up work on our 2006 application control reviews revealed that the Board had taken sufficient actions to allow us to close several open recommendations in this area.

To evaluate the Board's compliance with FISMA and related policies and procedures, we followed up on the open recommendations from our prior 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, other audit reports with information security-related recommendations. Based on our follow-up work, we determined that the Board's actions over the past year were sufficient to close seven of the ten recommendations that were not fully closed as of the beginning of our 2007 information security audit.

We also collected and reviewed information concerning the Board's processes related to areas for which the Office of Management and Budget (OMB) requested a specific response as part of the agency's annual FISMA reporting. Areas we reviewed include security awareness and training, certification and accreditation, remedial action monitoring, incident response, configuration management, controls over personally identifiable information, and privacy impact assessment processes.

Overall, we found that the Board's information security program continues to evolve and mature. The Board has made additional progress toward implementing a structured information security program as outlined by FISMA and has taken action to address open audit recommendations. Specifically, we found that the Board revised its information security program to incorporate guidance and standards recently issued by NIST. The Board also updated many of its information security policies and guidance, continued to certify and accredit information systems, and provided training to system owners and developers on their security-related responsibilities. Despite this progress, however, the Board still has work remaining to fully implement its information security program for all systems on the application inventory; consequently, three of our prior audit recommendations remain open or partially closed.

Based on our security-related fieldwork over the past year, we did not make any new recommendations in our report. In our opinion, the primary challenge going forward for the Board's Chief Information Officer (CIO) and Information Security Officer (ISO) is to ensure that all aspects of the revised information security program are fully and consistently implemented across the systems supporting divisions and offices—as well as for third-party applications supporting Board programs and operations—and that controls are implemented correctly, working as intended, and producing the desired results. We will continue to review the qualitative aspects of the program as part of future FISMA audits and evaluations.

We provided our draft report to the Director of the Division of Information Technology (IT), in her capacity as CIO for FISMA, and discussed the report with her and the Board's ISO at our closing meeting. During the meeting, the Director generally agreed with the report's contents. She and the ISO also discussed ongoing and planned activities to further enhance the Board's information security program.

Audit of the Board's Financial Statements for the Year Ended December 31, 2006

Each year, we contract for an independent public accounting firm to audit the financial statements of the Board. KPMG LLP, our contracted auditors for the 2006 financial statements, planned and performed the audit to obtain reasonable assurance that the financial statements were 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's audit and issued the audit report. In the auditors' opinion, the Board's financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2006; 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 a matter involving internal controls over financial reporting that they considered to be a significant deficiency. The matter related to controls over recording disbursement transactions, posting accrued leave, billing and monitoring receivables, recording property transactions, and preparing financial statement disclosures.

As part of obtaining reasonable assurance about whether the financial statements were 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 that are required to be reported under *Government Auditing Standards*.

ONGOING AUDIT WORK

Expenditure Assessment Control Review

Section 10 of the Federal Reserve Act allows the Board to levy a semiannual assessment on the Federal Reserve Banks to defray its estimated expenses, including the salaries of the members and employees of the Board. The assessment is one of the largest line items on the Board's annual financial

statements. For calendar year 2006, the assessment was approximately \$300 million.

Earlier this year, we began a review to evaluate the effectiveness of the Board's controls over the process for levying the expenditure assessment. Specifically, we are assessing whether the Board's controls are designed properly and operate effectively in order to provide reasonable assurance that (1) records and transactions are maintained in sufficient and accurate detail to permit the preparation of financial statement information in accordance with Generally Accepted Accounting Principles (GAAP); (2) transactions are processed in compliance with applicable laws and regulations and management's authorization; and (3) unauthorized or fraudulent transactions are prevented or can be detected in a timely manner. We are reviewing supporting documentation, and have interviewed Board and Reserve Bank management and staff, developed process flowcharts and narratives, identified and tested key process controls, and prepared a risk control matrix. We expect to issue our final report early in the next reporting period.

Currency Expenditure and Assessment Control Review

In April 2007, we began a control review of the Board's processes for recording expenses associated with currency (such as printing, issuance, and shipping) and for levying assessments on the Reserve Banks for these expenses. We began this review because the dollar value of the expenses and the corresponding assessments—almost \$492 million each in 2006—are the largest line items on the Board's financial statements. Our review objective is to evaluate the effectiveness of the Board's controls over these processes. Specifically, we plan to assess whether the Board's controls are designed and operate effectively to provide reasonable assurance that (1) records and transactions are maintained in sufficient and accurate detail to permit the preparation of the Board's financial statement information in accordance with GAAP; (2) financial transactions are processed in compliance with applicable laws and regulations and management's authorization; and (3) unauthorized or fraudulent financial transactions are prevented or can be detected in a timely manner.

During this reporting period, we developed process flowcharts and narratives, identified key process controls, and assembled a risk control matrix. Our work included interviewing Board and Reserve Bank management and staff, as well as staff at the U.S. Department of Treasury's Bureau of Engraving and Printing. We plan to begin testing controls early in the next reporting period and will present our results to management once testing is completed.

Management and Accountability of Mobile Computing Devices

Earlier this year, we began an audit of the management and accountability of mobile computing devices used by the Board. We are performing this audit as a follow-on to previous audit work related to the Board's management of fixed assets, as well as the result of recent government-wide interest in, and concerns over, personally identifiable information. Our objective is to evaluate controls over the receipt, tracking, securing, and disposal of selected mobile computing devices. We are focusing our audit work on controls related to laptops, Blackberry devices, and thumb/jump drives.

To accomplish our objective, we surveyed all Board divisions and offices regarding their use of mobile computing devices and used the survey results to select several divisions for detailed testing. We are flowcharting division processes, identifying key controls, and then testing those controls. We also plan to benchmark other organizations to identify any established best practices.

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.

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

During this period, we completed an inspection of the Board's Protective Services Unit (PSU), the organization that ensures the physical security of the Chairman of the Board of Governors. The USA PATRIOT Act of 2001 granted the Board certain federal law enforcement authorities, and the regulations implementing this new authority—the *Uniform Regulations for Federal Reserve Law Enforcement Officers* (Uniform Regulations)—designated the OIG as the External Oversight Function (EOF) for the Board's law enforcement programs. We performed this inspection to fulfill our EOF responsibility.

The objective of this inspection was to provide reasonable assurance that the PSU complied with the Uniform Regulations, Board and PSU internal policies and procedures, and applicable laws. To accomplish our objective, we performed a comprehensive inventory of PSU weapons and ammunition, reviewed training and personnel records for PSU management and staff, and verified that PSU law enforcement officers obtained required certifications. Also, we interviewed Board and PSU management and staff, as well as law enforcement officials at the United States Secret Service and another federal agency that has a personal protection function.

Overall, we found that the PSU generally complies with the Uniform Regulations, Board and PSU internal policies and procedures, and applicable laws. The inspection report included three recommendations designed to enhance PSU's internal control environment. We presented the inspection results to the Staff Director for Management and the PSU Special Agent in Charge who concurred with our findings and agreed to implement our recommendations. Our report will not be made available to the public because it contains security-related information.

Inspection of Federal Reserve Examination Practices for Assessing Financial Institutions' Office of Foreign Asset Control Compliance Programs

We also completed an inspection of Federal Reserve Examination Practices for Assessing Financial Institutions' Office of Foreign Asset Control (OFAC) compliance programs. OFAC, an entity within the U.S. Department of the Treasury, administers and enforces economic and trade sanctions against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. Although not required by specific regulation, financial institutions are expected to maintain a written, risk-focused program of compliance with OFAC requirements as a matter of sound banking practice. While federal bank regulatory agencies do not have a primary role in identifying OFAC violations, they are responsible for evaluating the sufficiency of policies, procedures, and processes that a bank follows to comply with OFAC laws and regulations. Federal Reserve examiners perform OFAC reviews as part of the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) assessments that they conduct during safety and soundness examinations. The Federal Financial Institutions Examination Council's *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (Manual) establishes the principles and procedures governing OFAC reviews.

The objective of this inspection was to assess Federal Reserve examiners' compliance with the OFAC examination guidance set forth in the Manual. We conducted our fieldwork at the Board and three Federal Reserve Banks—Atlanta, New York, and San Francisco—and selected a judgmental, representative sample of OFAC examinations based on criteria that included geography, asset size, and degree of international exposure. Out of a universe of 420 examinations performed from September 1, 2005, through June 1, 2006, we selected forty-nine examinations to be reviewed. The sample included state member banks, bank holding companies, Edge Act corporations, foreign banking organizations, and institutions with BSA/AML or OFAC programs that were rated as inadequate. These institutions had asset sizes ranging from \$7 million to \$500 billion.

In general, we found that Federal Reserve examiners were performing OFAC reviews in accordance with the guidance contained in the Manual, and in a manner that was commensurate with the financial institution's BSA/AML and OFAC risk profiles. Examination workpapers contained documentation indicating that examiners reviewed OFAC-related policies and procedures, risk assessments, the results of transaction testing, and prior deficiencies identified by OFAC, bank internal and external auditors, or regulators. Accordingly, nothing came to our attention to indicate material examiner noncompliance with the guidance contained in the Manual, and we concluded our work without making any recommendations. We discussed the results of our inspection with senior staff members in the Division of Banking Supervision and Regulation (BS&R) prior to issuing the final report.

ONGOING INSPECTIONS AND EVALUATIONS

Evaluation of the Board's Certification and Accreditation Process

The OIG is currently conducting an evaluation of the Board's certification and accreditation (C&A) process. FISMA directed NIST to establish guidelines for ensuring the security of federal information systems. As part of this responsibility, in May 2004, NIST developed *Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems*, to provide guidelines for the security certification and accreditation of government information systems. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. Security accreditation provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective information system security controls possible. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a security breach occurs.

The objective of this project is to evaluate the Board's C&A process and determine the extent to which it fulfills the NIST guidelines for evaluating security controls and protecting IT systems. The results of this evaluation will also be used as part of our overall evaluation of the Board's information security program, as required by FISMA.

Inspection of Reserve Bank Controls for Protecting Personally Identifiable Information Collected During Bank Examinations

We are currently conducting an inspection of Reserve Bank controls over personally identifiable information (PII) that is collected during the bank examination process. The Divisions of Consumer and Community Affairs (C&CA) and BS&R support and oversee the supervisory efforts of the Federal Reserve Banks to ensure that consumer protection laws and regulations are fully and fairly enforced, as well as to ensure the safety and soundness of state member banks. To fulfill their mission, Federal Reserve examiners access and analyze bank data that may include PII.

Government-wide measures to safeguard PII were included in OMB guidance that requires agencies to train employees and establish administrative, technical, and physical safeguards to protect the security and integrity of confidential records. The guidance is designed to prevent unauthorized disclosures of PII that could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual. OMB also requires agencies to apply safeguards to assure that sensitive agency information is protected. Those requirements include actions to protect sensitive information processed on computers and related hardware.

In response to OMB guidance, C&CA and BS&R issued procedures entitled, “Safeguarding and Reporting a Loss of Confidential Information and Assets,” that highlight requirements and guidance for safeguarding confidential information in hard copy and digital form, including information stored on electronic hardware such as workstations, laptops, and removable media such as Blackberry devices, thumb drives, CDs, and DVDs.

The objective of our review is to evaluate the Reserve Banks’ examination policies, procedures and controls, and examiner practices for safeguarding PII to ensure compliance with OMB directives and guidance issued by the Board. In addition, to address Board senior management interest in best practices at other agencies, we will visit federal bank regulatory and other agencies to determine whether there are any best practices that could be adopted by the Federal Reserve. In particular, we will review what these other regulators and agencies do to protect sensitive confidential information (in electronic and hard copy form) while it is being (1) transported to and from the office; and (2) used at alternative worksites such as residences.

Inspection of Examination Procedures for Financial Institutions with High Concentrations of Commercial Real Estate

Losses in bank commercial real estate (CRE) portfolios played a central role in the banking problems experienced during the late 1980s and early 1990s. Over the past several years, federal bank regulatory supervisors observed that CRE concentrations have been rising at many banks, especially small- to medium-sized institutions. While it appears that most bank underwriting practices are sound, supervisors became concerned that some institutions' risk management practices and capital levels had not evolved with the level and nature of their CRE concentrations.

In December 2006, in response to these concerns, supervisors issued interagency guidance entitled, “Concentrations in Commercial Real Estate Lending, Sound Risk Management Practices.” The intent of this guidance was to remind institutions that strong risk management practices and appropriate levels of capital are important elements of a sound CRE-lending program, especially when an institution has a CRE concentration or a CRE-lending strategy leading to a concentration. The guidance provides a principle-based discussion of supervisory expectations for sound risk management practices and for evaluation of capital adequacy.

We have begun a scoping effort to review Federal Reserve examinations of institutions with high CRE concentration levels, focusing on those examinations that were conducted after the new guidance was issued. We will further refine this objective once our scoping work is completed.

Evaluation of Data Flows for Board Employee Data Received by the Office of Employee Benefits and its Contractors

The Board's 2005 Financial Statement Audit revealed discrepancies between the Board's human resources database and the data used by the Board's actuary to determine pension benefit liability. In addition, during our 2005 evaluation of service credit computations, we found data discrepancies between the Board's information system and the system maintained by an Office of Employee Benefits (OEB) contractor that serves as the record keeper for the Federal Reserve System's Retirement, Thrift, Long-Term Disability, and Supplemental Survivor Income plans.

In light of these findings, we are conducting an evaluation of the controls over data flowing from the Board to OEB and its contractors. The objective is to determine the adequacy and effectiveness of controls over Board employee information that is received, processed, and disseminated by the OEB and its contractors. As part of this effort, we are also following up on the three recommendations made in our August 2005 report, *Evaluation of Service Credit Computations*.

Investigations

The Investigations program conducts criminal and administrative investigations in support of 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 of criminal procedure, as well as other rules, regulations, and court decisions governing the conduct of criminal, civil, and administrative investigations. Additionally, OIG special agents obtain authority to exercise specific law enforcement powers through a blanket deputation agreement with the Department of Justice (U.S. Marshals Service).

As major economic and financial trends continue to shape the environment in which the Board and other financial regulatory agencies operate, the challenges faced by financial regulators to implement new requirements for banks to detect illegal activities—such as money laundering and terrorist financing—also continue to evolve. As a result, the nature and complexity of our investigations continue to change. During this reporting period, our criminal investigative activity involved leading or participating in multi-agency task forces where alleged bank fraud, terrorist financing, and money laundering were among the crimes being investigated. In addition, OIG 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 activity over the last six months:

Alleged Prime Funds Bank Fraud

As previously reported, the OIG received a request from the U.S. Secret Service for assistance with a criminal investigation regarding a prime funds bank fraud case involving a private hedge fund manager and a board of directors member of an institution regulated by the Federal Reserve System. The scheme to defraud the hedge fund manager of \$25 million was perpetrated, in part, by using the Federal Reserve's name and claiming that the fictitious investments were overseen by a "Federal Reserve Administrator."

On November 12, 2005, the now-former director of the institution and two associates were arrested and charged with wire fraud. The complaint filed by the U.S. Attorney's Office charged the individuals with having made false statements to a hedge fund manager so that they could keep the \$25 million invested with a Nevada-based company. The investigation resulted in a \$22.4 million recovery (in a prior reporting period) of funds defrauded from the hedge fund manager. During the current reporting period, one of the individuals pleaded guilty to one count of attempting to impede, obstruct, and influence an investigation. A trial date has been scheduled for another individual, and we are continuing to work jointly with the U.S. Secret Service and the cognizant Assistant United States Attorney.

Alleged Conflicts of Interest by a Former FRB Employee

During the current reporting period, the OIG completed an investigation of a possible conflict of interest by a former Board employee. The OIG initiated the investigation after receiving two complaints alleging possible conflict of interest and self-dealing by the former Board employee with respect to the employee's relationship to a particular bank at the time the employee accepted a position with that same bank. The investigation found no evidence to substantiate that the former employee violated any federal laws or regulations governing either post-employment by former officers, employees, and elected officials, or acts affecting a personal financial interest.

Alleged Misuse of the Government Travel Card

During this reporting period, the OIG completed an investigation involving allegations of improper use of a Government Travel Card (GTC) by a Board employee. The OIG initiated this investigation in response to a referral from the Board that the employee misused the GTC after receiving a warning in March 2007 for using the GTC inappropriately for cash advances and rental car expenses in the Washington, D.C. area. The investigation confirmed that, after receiving the warning, the employee obtained numerous cash withdrawals and made other charges which appeared to be questionable and unrelated to Board travel. On September 28, 2007, the OIG issued a letter report to the cognizant division director for appropriate administrative action.

Summary Statistics on Investigations for the Period April 1 through September 30, 2007

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	5
Investigations Open from Previous Period	12
Investigations Closed during Reporting Period	5
Total Investigations Active at End of Reporting Period	12
Investigative Results for this Period	
Referred to Prosecutor	0
Joint Investigations	8
Referred for Audit	1
Referred for Administrative Action	1
Oral and/or Written Reprimand	0
Terminations of Employment	0
Arrests	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

The OIG received 122 complaints from hotline calls, correspondence, e-mail, facsimile communications, requests from Federal Reserve System employees, and members of the public. All complaints received were evaluated to determine if further inquiry was warranted. Most hotline contacts were from consumers with complaints or questions about the practices of financial institutions. Other hotline contacts were from individuals seeking advice about programs and operations of the Board, Federal Reserve Banks, other Offices of Inspector General, and other financial regulatory agencies. These inquiries were referred to the appropriate Board offices, Reserve Banks, or federal or state agencies.

The OIG continued to receive a significant number 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 following table:

Summary Statistics on Hotline Results for the Period of April 1 through September 30, 2007

Hotline Complaints	Number
Complaints pending from the previous reporting period	7
Complaints received during this reporting period	122
Total complaints for the Reporting Period	129
Complaints resolved during this period	123
Complaints pending	6

Legal Services

During this semiannual reporting period, the Legal Services Program provided comprehensive legal advice, research, counseling, critical analysis, and representation in support of the OIG projects and activities (that is, OIG management, audits, investigations, inspections, evaluations and other professional and administrative functions.) This work often provides the legal basis for conclusions, findings, and recommendations in OIG reports. In addition, Legal Services keeps the IG and OIG staff aware of recent developments in the law that may affect the activities of the OIG and the Board. The following illustrates selected highlights of Legal Services' work during this reporting period, as well as certain ongoing projects:

- research and analysis regarding the Board's compliance with FISMA, specifically regarding issues related to the handling of PII and questions concerning the requirements associated with Privacy Impact Assessments;
- legal review and advice concerning access to agency records under the IG Act;
- tracking, analysis, and comments regarding various legislative proposals to significantly amend the IG Act of 1978;
- interpretation of contract clauses with respect to the OIG's contracts for the Board's financial statement audit;
- research and analysis regarding the legal requirements concerning Reserve Bank and currency expenditure assessments;
- research, analysis, and advice concerning the use of video surveillance for investigative purposes;
- legal advice and support regarding OIG personnel matters;
- professional training sessions to OIG staff concerning PII, Advice of Rights, and the IG Act;
- legal analysis and advice concerning financial conflicts of interest;
- review and comments concerning various Board policies, including: the Premium Pay Policy, the implementation of the Fair Labor Standards Act, Suitability Determinations Policy, various Board policies relating to the handling of privacy information, and the revised Travel Policy;
- legal review and response to Freedom of Information Act and Privacy Act requests; and
- compilation of criminal law provisions relating to bank fraud and money laundering, as well as other associated statutes.

Involvement in the larger OIG community continues to play an important role in Legal Services' activities. OIG attorneys remained active in the Council of Counsels to the Inspector General (CCIG). We also continue to work with the IG community's Legislation Committee on a variety of matters potentially affecting the community. Legal Services has also played a significant role in the development of a website that will service the entire community of OIG attorneys.

Pursuant to the IG Act, as amended, the Legal Services staff conducts independent reviews of new and proposed legislation and regulations to determine their potential effect on the economy and efficiency of the Board's programs and operations. During this reporting period, Legal Services reviewed thirty-six legislative and regulatory items. The following table contains selected highlights of our work in this area:

Highlights of the OIG's Review of Laws and Regulations, April 1 through September 30, 2007

Board/Banking Legislation	
Legislation Reviewed	Purpose/Highlights
Federal Housing Financing Reform Act of 2007 (H.R. 1427)	Seeks to reform the regulation of certain housing-related Government-sponsored enterprises, and for other purposes.
CTR [Currency Transaction Report] Modernization Act (H.R. 1447)	Amends certain requirements for reporting cash transactions, and for other purposes.
Freedom to Bank Act (H.R. 2096)	Sunsetts federal laws and regulations regarding control of bank accounts, and for other purposes.
Native American \$1 Coin Act (H.R. 2358)	Commemorates Native Americans and their contribution to the development of the United States, by minting and issuing \$1 coins.
Coinage Material Modernization Act of 2007 (H.R. 3330)	Provides authority to change the composition of coins issued by the U.S. Mint.
Sunshine in Monetary Policy Act (H.R. 2754)	Requires the Board to make available to the public, on a weekly basis, information on the measure of the M3 monetary aggregate, and its components, and for other purposes.

Highlights of the OIG's Review of Laws and Regulations, April 1 through September 30, 2007 (con't)

Consumer Protection and Information Security Legislation	
Legislation Reviewed	Purpose/Highlights
Borrower's Protection Act of 2007 (S. 1299)	Establishes on behalf of consumers a fiduciary duty and other standards of care for mortgage brokers and originators, and establishes standards to assess a consumer's ability to repay, and for other purposes.
Universal Default Prohibition Act of 2007 (S. 1309) (H.R. 2146)	Amends the Truth in Lending Act to prohibit universal defaults on credit card accounts, and for other purposes.
Federal Agency Data Breach Protection Act (S. 1558)	Amends title 44 of the United States Code to strengthen requirements related to security breaches of data involving the disclosure of sensitive personal information.
Identity Theft Protection Act of 2007 (H.R. 3316)	Establishes a centralized procedure for customers to obtain a security freeze on their consumer credit reports from the major credit reporting firms.
Identity Theft Notification Act of 2007 (H.R. 136)	Amends Title II of the Social Security Act to require the Commissioner to notify individuals and appropriate authorities of evidence of misuse of an individual's Social Security Number.
Federal Agency Data Mining Reporting Act of 2007 (S. 236)	Requires reports to Congress on federal agency use of data mining.
Social Security Number Misuse Prevention Act (S. 238)	Amends title 18 of the United States Code in order to curtail the misuse of Social Security numbers, and provides for civil and criminal penalties.
Notification of Risk to Personal Data Act of 2007 (S. 239)	Requires any agency or business involved in interstate commerce that uses or stores sensitive personally identifiable information to notify any U.S. residents whose information may have been improperly accessed or acquired.
Personal Data Privacy and Security Act of 2007 (S. 495)	Seeks to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, enhances criminal penalties, provides law enforcement assistance, and creates other protections against security breaches, fraudulent access, and misuse of personally identifiable information.
Social Security Number Protection Act of 2007 (H.R. 948)	Increases authority of the federal government to protect individuals from certain acts and practices in the sale and purchase of Social Security numbers.
Data Security Act of 2007 (S. 1260)	Seeks to protect information relating to customers, to require notice of security breaches, and for other purposes.
Credit Agencies Identity Theft Responsibilities Act of 2007 (H.R. 2568)	Amends the Fair Credit Reporting Act to establish additional reporting requirements to enhance the detection of identity theft.

Highlights of the OIG's Review of Laws and Regulations, April 1 through September 30, 2007 (con't)

Inspector General and Law Enforcement Legislation	
Legislation Reviewed	Purpose/Highlights
Combating Money Laundering and Terrorist Financing Act of 2007 (S. 473)	Closes various gaps in the criminal law regarding money laundering statutes, increases penalties in certain areas, and expands the investigatory power of the Secretary of Homeland Security.
Transparency and Accountability in Security Contracting Act of 2007 (H.R. 369)	Requires accountability for personnel performing private security functions under federal contracts, and for other purposes.
A bill to grant immunity from civil liability to any person who voluntarily notifies appropriate security personnel of suspicious activity believed to threaten transportation safety or security or takes reasonable action to mitigate such activity (S. 1369)	Grants immunity from civil liability to any individual who voluntarily notifies appropriate security personnel of suspicious activity believed to threaten transportation safety.
Accountability in Government Contracting Act of 2007 (S. 680)	Seeks to ensure proper oversight and accountability in Federal contracting, and amends the Inspector General Act of 1978 to enhance the independence of the Inspectors General.
Improving Government Accountability Act (H.R. 928 and S. 1723)	Amends the Inspector General Act of 1978 to enhance the independence of the Inspectors General and to create a statutory unified Council of the Inspectors General on Integrity and Efficiency, and for other related purposes.
Government Accountability Office Act of 2007 (H.R. 3268)	Amends the appointment process of the Comptroller General and Deputy Comptroller General at GAO and creates a statutory Office of Inspector General at GAO, among other purposes.

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 the broader IG and professional communities and promote coordination on shared concerns. Within the Board and the Federal Reserve System, we continue to share information about our roles and responsibilities. Highlights of our activities follow:

Executive Council on Integrity and Efficiency (ECIE) Participation

The Board's IG serves as a member of the ECIE, which was created by Executive Order in 1992 to facilitate coordination among IGs of designated federal entities. Collectively, the members of the ECIE work with the members of the President's Council on Integrity and Efficiency (PCIE) to help improve Government programs and operations. The PCIE and ECIE provide a forum to discuss government-wide issues and shared concerns. The Board's IG was recently appointed to serve as a representative to the Legislation Committee, which serves as the central point of information regarding legislative initiatives and congressional activities that may affect the community. In this role, the Board's IG helps to keep the PCIE and ECIE informed about relevant bills and amendments that would affect IG statutory authority or create new IG responsibilities.

Financial Regulatory OIG Coordination

To foster collaboration and cooperation on issues of mutual interest, the Board's IG meets regularly with the IGs from other federal financial regulatory agencies: the Federal Deposit Insurance Corporation, the Department of the Treasury, the National Credit Union Administration, the Securities and Exchange Commission, the Farm Credit Administration, the Commodity Futures Trading Commission, and the Federal Housing Finance Board. At the same time, the Assistant IG for Audits and Attestations and the Assistant IG for Inspections and Evaluations also meet with their OIG counterparts from these agencies to discuss and coordinate issues of interest, annual plans, and ongoing projects.

Committee, Workgroup, and Program Participation

The IG also serves on various Board committees and work groups, such as the Space Planning Executive Group and the Senior Management Council. In addition, IG staff participate in a variety of Board working groups, including the Leading and Managing People (LAMP) Working Group, the Information Technology Advisory Group (ITAG), the Board's Core Response Group, the Management Advisory Group (MAG), and the Board's Continuity of Operations

(COOP) Working Group. The OIG is also an active participant in other Board-sponsored programs. For example, during the current reporting period, the IG, Assistant IG for Legal Services, and Legal Services staff addressed the Board's interns as part of the Board summer intern program. The IG and the Assistant Inspector General for Audits and Attestations also provided an overview of the OIG and discussed ongoing and planned work with General Auditors from across the Federal Reserve System at their July 2007 Conference of General Auditors meeting.

Council of Counsels to the Inspector General Summer Legal Intern Program

IG Legal Staff planned and coordinated a government-wide OIG Summer Legal Intern Program. This program—supported and assisted by IG Counsels from other agencies—was designed to provide the legal interns of the OIG community with information concerning the Inspector General history, mission, and legal framework, and to enrich the OIG-wide intern experience with the federal government. Approximately twenty-five summer legal interns from ten Offices of Inspector General participated in the program. This program also included various presentations and events designed to promote government service as a career. For example, arrangements were made for the interns to visit the United States Supreme Court and meet with the Clerk of the Court, to tour Capitol Hill and hear a panel of former congressional staffers currently working as lawyers in OIG offices, and to attend presentations by various Inspectors General and by U.S. Department of Justice and OIG attorneys concerning legal careers in the OIG community and the federal government generally.

IT Infrastructure Enhancements

During this reporting period, the OIG completed a significant update of our IT-related policies and procedures, and consolidated this guidance and supporting documentation into a central, IT infrastructure database. Through coordination with Board procurement, we recently contracted for a security certification of the OIG's IT infrastructure which will be conducted during the next reporting period. We anticipate that having a central repository of IT standards, profiles, inventories, and other documentation will help us to ensure FISMA compliance.

Appendixes

Appendix 1
Audit Reports Issued with Questioned Costs for the Period April 1 through
September 30, 2007

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, 2007

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
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 Information Security Program	09/04	5	5	0	09/07	5	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	09/07	1	0
Audit of the Board's Fixed Asset Management Process	05/05	2	2	0	03/06	1	1
Evaluation of Service Credit Computations	05/05	3	3	0	03/07	1	2
Audit of the Supervision and Regulation Function's Efforts to Implement Requirements of the Federal Information Security Management Act	09/05	4	3	1	09/07	3	1
Audit of the Board's Information Security Program	10/05	2	2	0	09/07	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	09/07	1	0
Audit of the Board's Information Security Program	09/06	2	2	0	09/07	2	0
Audit of the Board's Payroll Process	12/06	7	7	0	–	–	–
Audit of the Board's Compliance with Overtime Requirements of the Fair Labor Standards Act	03/07	2	2	0	–	–	–
Inspection of the Board's Protective Services Unit	09/07	3	3	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	18-20
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	15
5(a)(5)/6(b)(2)	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	25
5(a)(9)	Statistical Table—Recommendations that Funds Be Put to Better Use	26
5(a)(10)	Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made	27
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*

