Office of Inspector General Semiannual Report to Congress

October 1, 2007 – March 31, 2008

Board of Governors of the Federal Reserve System

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

OFFICE OF INSPECTOR GENERAL

April 29, 2008

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, 2007, through March 31, 2008. 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

October 1, 2007 – March 31, 2008

OIG

Office of Inspector General

Table of Contents

Introduction

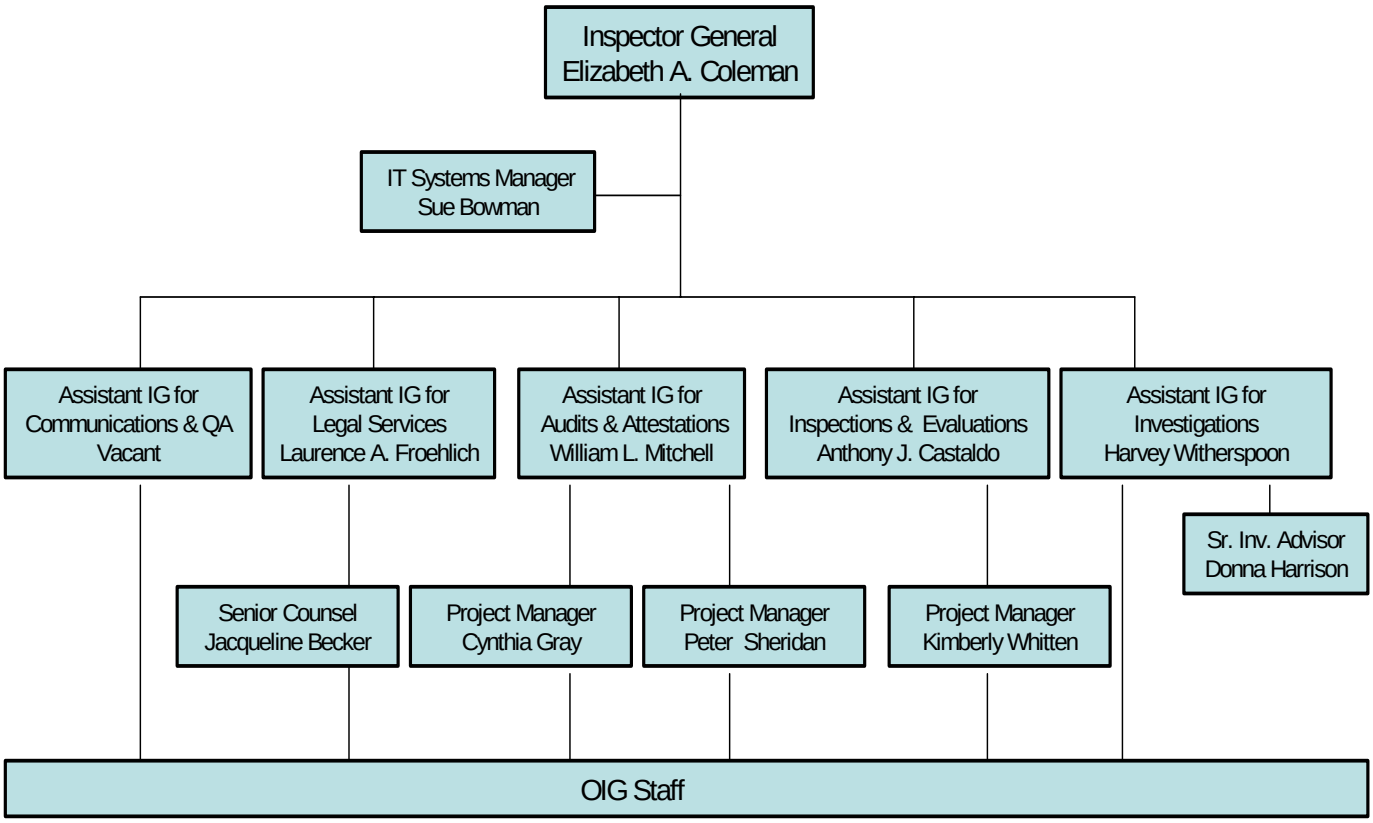
Consistent with the Inspector General Act of 1978 (IG Act), as amended, 5 U.S.C. app, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- 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 (now, the Deposit 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. In addition, the USA PATRIOT Act of 2001, Public Law 107-56 (October 26, 2001), grants the Board certain federal law enforcement authorities. Our office serves as the External Oversight Function for the Board's law enforcement program and operations.

OFFICE OF INSPECTOR GENERAL

April 2008



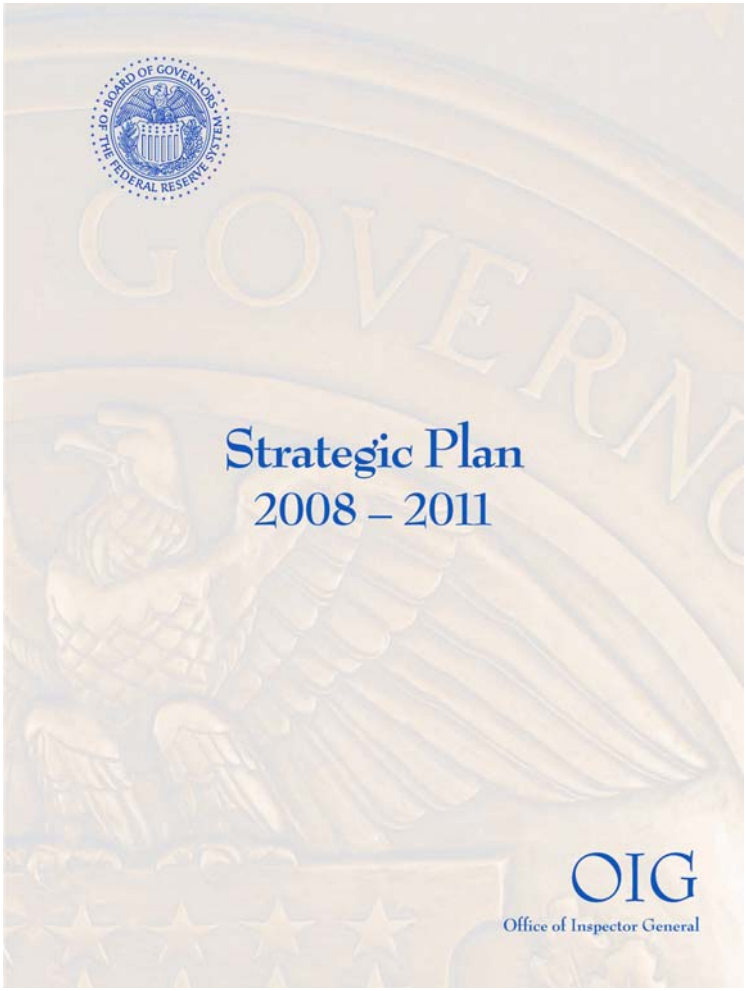
OIG Staffing

Auditors	**17**
Information Technology Auditors	**6**
Investigators	**5**
Attorneys	**3**
Administrative	**3**
Information Systems Analysts	**3**
Total Authorized Positions	**37**

Goals and Objectives

Strategic Plan

During the current reporting period, the OIG issued its Strategic Plan for 2008 through 2011. The Strategic Plan sets a results-oriented, risk-focused vision for our office, and describes the six fundamental values—independence, integrity, excellence, professionalism, empowerment, and commitment to the public interest—that will shape our decisions and day-to-day operations. As indicated in the overview on page 4, we will focus on achieving three primary goals: (1) conduct our statutorily legislated requirements; (2) broaden coverage of the Board's mission areas to enhance economy, limit risk, and detect and prevent fraud, waste, and abuse; and (3) enhance efficiency and effectiveness of the OIG's operations and communications. The plan sets specific objectives for each goal. In addition, we have established new performance indicators that will help us assess our accomplishments going forward.



Overview of the OIG's Strategic Plan, 2008 – 2011

MISSION

Support the Board in achieving its mission by conducting independent and objective audits, inspections, evaluations, investigations, and other reviews of Board programs and operations. Promote integrity, economy, efficiency, and effectiveness; help prevent and detect fraud, waste, and abuse; and help foster accountability to the Congress and the public.

VISION

The OIG strives to achieve results, assess risk, and protect the public interest through an independent partnership with the Board, built on integrity, excellence, and professionalism.

VALUES

Independence **Integrity** **Excellence** **Professionalism**

Empowerment **Public Interest**

GOAL 1

Conduct Work Consistent with the OIG's Statutory and Legislative Requirements

Objectives

- Conduct financial statement and internal control audits.
- Complete material loss reviews of bank failures.
- Conduct annual reviews of the Board's information security program.
- Provide external oversight of the Board's law enforcement activities.
- Review proposed legislation.
- Conduct criminal, civil, and administrative investigations.

GOAL 2

Broaden Coverage of Board Mission Areas to Enhance Economy, Efficiency, and Effectiveness; Limit Risk; Detect and Prevent Fraud; and Ensure Compliance

Objectives

- Enhance understanding of the Board's monetary policy function and plan work to add value.
- Address current and emerging challenges to the Supervision and Regulation function.
- Review oversight of Reserve Banks and efforts to foster efficiency and effectiveness of payment systems.
- Assess the integrity, efficiency, and effectiveness of the Board's internal administration and operations.
- Address cross-cutting issues.

GOAL 3

Enhance the Efficiency and Effectiveness of the OIG's Operations and Communications

Objectives

- Strengthen our human resource management.
- Enhance internal and external communication, coordination, and information sharing.
- Continue to improve our business processes.
- Continue to build our technology infrastructure.

AUDITS & ATTESTATIONS
Financial/Performance Audits
Attestation Engagements

INSPECTIONS & EVALUATIONS
Inspections/Program Evaluations
Best Practice Reviews

INVESTIGATIONS
Criminal/Civil Cases
Fictitious Instruments

LEGAL SERVICES
Legislative Review Regulation Review Policy Review Program and Project Legal Support

COMMUNICATIONS AND QUALITY ASSURANCE (QA)
Semiannual and Other Reports QA and Peer Review Routine Activities Internal Operations

Audits and Attestations

The Audits and Attestations program assesses 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. OIG audits and attestations are performed according to *Government Auditing Standards* established by the Comptroller General and mandated by the IG Act. 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 Financial Statements for the Year Ended December 31, 2007, and Audit of the Federal Financial Institutions Examination Council's Financial Statements for the Year Ended December 31, 2007

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 provides the accounting function for the FFIEC. Deloitte & Touche 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.

In the auditors' opinions, the Board's and the FFIEC's financial statements present fairly, in all material respects, the financial position of each as of December 31, 2007, and the results of operations and cash flows for the year then ended, in conformity with accounting principles generally accepted in the United States of America. To determine the auditing procedures needed to express an opinion on the financial statements, the auditors considered the Board's and the FFIEC's internal controls over financial reporting. Although the auditors' consideration of the internal controls would not necessarily disclose all matters that might be material weaknesses, no material weaknesses were noted. However, the auditors cited a matter involving internal controls over financial reporting that they considered to be a significant deficiency for the Board and the FFIEC. The matter related to logical access controls within the Board's general computer control environment.

As part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, the auditors also performed tests of the Board's and FFIEC's compliance with certain provisions of laws, regulations, and contracts 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 would be required to be reported under *Government Auditing Standards*.

Control Review of the Reserve Bank Operating Assessment Process

Section 10 of the Federal Reserve Act allows the Board to levy a semiannual operating assessment on the Federal Reserve Banks. The assessment should be sufficient to pay the Board's estimated operating expenses and capital expenditures for the half-year following the levying of such assessment, together with any deficit carried forward from the preceding half-year. The assessment is one of the largest line items on the Board's annual financial statements. For calendar year 2006, the assessment was approximately $301 million and for 2007 it was about $296 million.

During this reporting period, we completed a review to evaluate the effectiveness of the Board's controls over the process for levying the operating assessment on the Reserve Banks. Specifically, we assessed whether the Board's controls are designed and operated 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 generally accepted accounting principles, (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. To accomplish our objective, we reviewed supporting documentation, 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.

Overall, we found that the controls over the process for levying the operating assessment were generally effective. The documentation we reviewed was sufficient to permit the proper preparation of the Board's financial statements, and nothing came to our attention to indicate any instances of fraud, unauthorized transactions, or noncompliance with applicable laws and regulations. Although we found that controls are generally effective, our fieldwork also identified several opportunities to enhance controls related to documenting procedures, better aligning roles and responsibilities, recording journal entries in a more timely manner, and strengthening certain supporting documentation. We shared our observations with management, who proactively implemented changes that addressed these observations. As a result, we did not issue any formal

recommendations. However, we issued a management letter that included one suggestion for establishing greater consistency in the operating assessment process.

Information Security Control Reviews

Each year, the OIG conducts an audit of the Board's Information Security Program and practices pursuant to FISMA. To meet FISMA's requirement that the OIG evaluate the effectiveness of the information security control techniques for a subset of the agency's information systems, we performed security control reviews of two major applications: a bundle of subsystems referred to as the EGov Systems, and the Federal Reserve Integrated Records Management Architecture (FIRMA). Our objective, consistent with FISMA's requirements, was to evaluate the adequacy of control techniques for protecting the systems' data from unauthorized access, modification, destruction, or disclosure.

To accomplish this objective, we developed a control assessment tool based on the security controls defined in the National Institute of Standards and Technology (NIST) Special Publication 800-53 Rev. 1, *Recommended Security Controls for Federal Information Systems*. This document provides a baseline of management, operating, and technical security controls for organizations to use in protecting their information systems. The controls are divided into "families" (such as access control, risk assessment, and personnel security) and include controls that can be categorized as system-specific or common (that is, applicable across agency systems). Consequently, although our focus was on evaluating the application-specific controls, we also assessed some of the security controls that affect Board-wide operations since most applications rely on these controls. Based on our reviews, we identified application-specific findings and recommendations that we provided to the appropriate division director for review and comment. We also identified opportunities for the Board's Information Security Officer (ISO) to strengthen common controls. Each of these restricted reports is summarized below.

Security Control Review of the EGov Systems

The EGov Systems, which include six subsystems, are listed as a major application on the Board's FISMA application inventory for the Office of the Secretary (OSEC). Collectively, the EGov Systems allow OSEC to process and distribute restricted information to the Board members, Board staff, and Reserve Bank staff. Overall, our review showed that controls within the EGov Systems were generally well-designed and well-implemented, and that controls in thirteen of the seventeen control families generally met the control objectives. However, we found that information security controls need to be strengthened in four of the

seventeen control families and we made eight recommendations to address these issues. The Director of OSEC accepted the recommendations and indicated that she will implement them as soon as practicable. She also noted alternative approaches to implementing two recommendations that, if implemented as described, will satisfy the intent of our recommendations.

Security Control Review of the Federal Reserve Integrated Records Management Architecture

FIRMA is also listed as a major application for OSEC on the Board's FISMA application inventory. The application converts paper Board records and electronically-uploaded documents into electronic records and manages them in compliance with federal records management laws and regulations. Overall, our review showed that information security controls in thirteen of the seventeen control families generally met the control objectives. However, we found that security controls need to be strengthened in four control families and made seven recommendations to address these issues. The Director of OSEC accepted the recommendations and indicated that she will implement them as soon as practicable. The response noted alternative approaches to implementing two recommendations that, if implemented as described, will satisfy the intent of the recommendations.

Common Controls Report

Based on our security control reviews, we also identified opportunities for the Board's ISO to enhance and enforce existing policies and procedures and to provide additional guidance for implementing security controls, thereby assisting all system owners in implementing the Board's Information Security Program. Our work identified opportunities to strengthen controls in four of the seventeen control families.

We recognize that the ISO and his staff have completed a significant amount of work over the past few years to develop a security program that complies with new NIST requirements. For example, the ISO developed and issued guidance to assist Board staff in implementing certain components of the program, such as completing risk assessments and security plans in preparation for system certifications and accreditations. In 2007, the security staff in the Board's Division of Information Technology (IT) also conducted training for system owners and developers; the training covered the requirements of the Board's Information Security Program and provided guidance on completing

required documentation. As the Board's Security Program evolves and matures, we believe that the ISO will need to continue providing oversight, training, and develop additional guidance for the program to remain effective. The report contains six recommendations to assist the ISO in this effort.

The director of IT, in her capacity as Chief Information Officer for FISMA, generally agreed with all of the recommendations and identified corrective action that has either been taken or is underway to enhance the control families highlighted in our report.

FOLLOW-UP ACTIVITIES

Over the past few months, the OIG conducted follow-up work on open recommendations related to several prior OIG audit reports. Our work allowed us to close three recommendations as shown below.

Audit of the Federal Reserve's Background Investigation Process

Our October 2001 report contained three recommendations designed to improve the Board's background investigation program. In December 2007, the Board issued a new *Suitability Policy* which provides an overview of the background investigation process, explains the reason for and frequency of investigations, and describes the types of investigations performed for different job families. This action allows us to close our first recommendation. To close our remaining recommendations, we plan to select a sample of contractors, summer interns, and temporary employees to determine whether the new procedures have been properly followed.

Audit of the Board's Payroll Process

Our December 2006 report contained seven recommendations designed to improve the overall efficiency and accuracy of the Board's payroll processes and to help ensure compliance with applicable laws and regulations. During this reporting period, we reviewed actions taken regarding our recommendation related to overtime pay for law enforcement personnel. Since we issued our report, the Staff Director for Management signed a memorandum that authorized payment of overtime to law enforcement personnel for preparation time (time to get in uniform, retrieve their weapons, etc.) and the Management Division (MGT) revised the general orders to clarify the procedures. We are therefore closing this recommendation. MGT is completing work on our other recommendations and we will continue to review the actions taken.

Audit of the Board's Compliance with Overtime Requirements of the Fair Labor Standards Act

Our March 2007 audit report contained two recommendations designed to enhance controls related to the Fair Labor Standards Act (FLSA) processing, as well as to better align the Board's policies and processes with FLSA requirements. The recently revised *Overtime and Other Forms of Premium Pay* policy addresses the concerns we highlighted in our report and allows us to close our second recommendation. Once MGT completes modifications to the Board's human resources management system to address our control-related concerns, we will perform additional follow-up work regarding our first recommendation.

ONGOING AUDIT WORK

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 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 item on the Board's financial statements. Our review objective is to evaluate the effectiveness of the Board's controls over these processes. Specifically, we will assess whether the Board's controls are designed and operating 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 generally accepted accounting principles, (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 completed testing of the process controls, including key controls, and discussed the results with management. Our testing was based on process flowcharts and narratives we developed through interviews of Board and Reserve Bank management and staff, as well as staff at the Department of the Treasury's Bureau of Engraving and Printing (BEP). We expect to issue our final report early in the next reporting period.

Management and Accountability of Mobile Computing Devices

In the first quarter of last 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 (PII). 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 Universal Serial Bus (USB) flash 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 prepared flowcharts of the divisions' processes, identified key controls, and, during the reporting period, completed testing of those controls. We also plan to perform benchmarking visits to other organizations to identify best practices. We expect to complete this project and issue our final report early in the next reporting period.

Security Control Review of the Currency Ordering System

During this period, we began a security control review of the Currency Ordering System (COS). COS, which includes two subsystems, is listed as a major application on the Board's FISMA application inventory for the Division of Reserve Bank Operations and Payment Systems. Collectively, these systems enable users from the Board, BEP, and the Federal Reserve Banks to monitor and control the production, inventory, and distribution of new currency throughout the United States; streamline and automate the billing process between the Board and the armored carrier companies that ship currency from BEP to the Federal Reserve Banks and branches; and maintain and track shipments that are transported from one Federal Reserve Bank to another. We have issued a draft report for management's review and comment and expect to issue our final report early in the next reporting period.

Security Control Reviews of two Federal Reserve Bank of Boston Applications

Late last year, we began security control reviews of two applications maintained by the Federal Reserve Bank of Boston: the Supervision, Regulation, and Credit (SRC) Infrastructure and a Lotus Notes Bundle. We selected the SRC Infrastructure and Notes Bundle because they have been classified as a general support system and a major third-party application, respectively, on the Board's FISMA application inventory under the Division of Banking Supervision and Regulation (BS&R). The SRC Infrastructure consists of various hardware and software components configured to provide information technology tools and support for Boston SRC operations. The Lotus Notes Bundle consists of two applications used to support bank examinations. We have finished our control testing and will present our results to management in a draft report early in the next reporting period.

Inspections and Evaluations

The Inspections and Evaluations program 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. OIG inspections and evaluations are performed according to *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE).

Inspection of Controls for Safeguarding Confidential and Personally Identifiable Information Collected During Bank Examinations

During the period, we completed an inspection of Reserve Bank controls for safeguarding confidential and sensitive information that includes PII collected during bank examinations. PII is information that identifies or describes a particular individual and may include an individual's name, birth date, account numbers, place of birth, driver's license number, passwords or security codes, or any other personal information that can be linked to an individual. Federal Reserve Banks conduct safety and soundness, and consumer compliance examinations at state-chartered member banks under delegated authority from the Board. During financial institution examinations, Reserve Bank staff access and analyze information that is confidential, sensitive, and may include PII. Reducing the risk of inappropriate or inadvertent disclosure of confidential and sensitive information, including PII, is vital because security breaches could have serious impacts on supervised institutions, their customers, and the Federal Reserve System. The objective of this inspection was to evaluate policies, procedures, practices, and controls to safeguard confidential supervisory information, including PII, collected during bank examinations (hereinafter, referred to as confidential information).

Government-wide measures to safeguard PII were included in recent Office of Management and Budget (OMB) guidance that requires agencies to train employees and establish administrative, technical, and physical safeguards to protect the security and integrity of confidential records. OMB also requires agencies to apply safeguards to protect sensitive agency information that is processed on computers and related hardware, and to meet certain security incident reporting requirements. In January 2007, BS&R and the Division of Consumer and Community Affairs (C&CA) issued procedures for safeguarding and reporting a loss of confidential information and assets (hereinafter, the procedures). To accomplish our inspection objective, we visited five Federal

Reserve Banks and performed specific tests to verify that supervision and regulation staff members were complying with the procedures.

In general, our inspection-related testing and observations revealed that the Reserve Banks we visited are complying with the procedures. In addition, we found that all of the Reserve Banks are providing training for safeguarding confidential information, and that staff were generally aware of requirements to ensure the security of confidential information contained in documents and equipment. Further, our inspections of document storage and other facilities indicated that Reserve Banks were securing, archiving, and disposing of documents and equipment in accordance with the procedures. While conducting our inspection fieldwork, we noted that several Reserve Banks initiated actions to protect computer equipment and confidential information that supplemented provisions included in the procedures. We listed these additional procedures in our restricted report because other Reserve Banks may find these initiatives useful for strengthening procedures in their respective districts.

During the course of our inspection, the Staff Director for Management expressed interest in other agencies' practices for reducing the risk of theft or loss of laptops and confidential information while employees are traveling or working outside of their offices. Because we also saw value in obtaining insights into other agencies' practices for safeguarding electronic devices and confidential information, we expanded the scope of our inspection and included visits to nine other agencies, four of which are federal financial regulators. We analyzed the materials obtained during our visits to derive the core requirements that other agencies have implemented to safeguard laptops and confidential information while employees are traveling or working outside of their offices, and compared these core requirements to the procedures. We found that the procedures cover almost all of the other agencies' core requirements. However, we noted two core requirements that the procedures do not address, and requested that the Directors of BS&R and C&CA review these requirements and consider adding them to the procedures. We also compared the other agencies' core requirements to the Board's policies and procedures for safeguarding laptops and confidential information, and plan to communicate the results of this analysis in a separate briefing to the Staff Director for Management.

FOLLOW-UP ACTIVITIES

Follow-up on the Review of the Board's Workers' Compensation Program

During this reporting period, we reviewed actions taken in response to the four recommendations made in our March 2005 report on the *Review of the Board's Workers' Compensation Program*. The Board implemented a variety of policies, procedures, and processes to enhance internal controls and program effectiveness. These measures included implementing a *Return-to-Work Policy* that provides

light-duty assignments for employees who cannot perform their regular duties, a process for analyzing accidents to prevent future occurrences, and a procedure for ensuring that workers' compensation cases are systematically reviewed for fraud. Our follow up work revealed that sufficient action has been taken to close all four recommendations.

Follow-up on the Inspection of the Board's Security Services Unit

Our March 2006, *Report on the Inspection of the Board's Security Services Unit* (currently known as the Law Enforcement Unit) contained three recommendations for improving the Law Enforcement Unit's internal controls and operations. Actions taken to fulfill our recommendations included a variety of policy enhancements designed to strengthen internal controls. In addition, the Federal Reserve's Basic Law Enforcement Training Program was accredited by the Federal Law Enforcement Training Accreditation Board in November 2007. We concluded that actions taken warranted closing all three recommendations.

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*, that provides 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 impact to the agency if a security breach occurs.

The project objective 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 information technology 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 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 agencies observed that CRE concentrations have been rising at many banks, especially small- to medium-sized institutions. In December 2006, in response to these concerns, the regulatory agencies 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 completed a scoping effort that focused on reviewing Federal Reserve examinations of institutions with high CRE concentration levels that were conducted after the new guidance was issued. We are reviewing the scoping phase data to determine the best approach for future evaluation work in this area.

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

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 OEB and its contractors.

Investigations

The Investigations program conducts criminal, civil, and administrative investigations in support of the Board's programs and operations. To effectively carry out its mission, OIG special agents 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 have authority to exercise specific law enforcement powers through a blanket deputation agreement with the Department of Justice' U.S. Marshals Service. OIG investigations are conducted in compliance with *Quality Standards for Investigations* issued by the PCIE/ECIE.

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 that were 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.

Guilty Verdict in Alleged Prime Bank Fraud Case

On November 20, 2007, the primary subject of this investigation was convicted on eleven counts of wire fraud in connection with a scheme to defraud a hedge fund manager and her investors of $25 million. As previously reported, the OIG participated in a joint investigation with the U.S. Secret Service of a "prime bank" fraud scheme involving a private hedge fund manager who was victimized by the primary subject, his associate, and a board of directors member of an institution regulated by the Federal Reserve System. The scheme to defraud the hedge fund was perpetrated, in part, by using the Federal Reserve's name and claiming that the fictitious investments were overseen by a "Federal Reserve Administrator."

In November 2005, the primary subject, his associate, and the now-former director of the institution were arrested and charged with wire fraud. During the last semiannual reporting period, the associate pleaded guilty to one count of attempting to impede, obstruct, and influence an investigation. The complaint filed by the United States Attorney's Office charged the individuals with having made false statements to the 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 (noted in a prior reporting period) of funds defrauded from the hedge fund manager.

The Federal Reserve has issued, in the past, alerts concerning illegal schemes purporting to involve "prime bank" financial instruments. The alerts have advised banking organizations and the public that, among other things, the Federal Reserve does not know of any legitimate use of any financial instrument called a "prime bank" note, guarantee, letter of credit, or debentures. In addition, the alerts made it clear that the Federal Reserve does not guarantee or enter into transactions with individuals and does not license anyone to trade "prime bank" financial instruments or act as the Federal Reserve agent to sell or redeem such instruments.

This case was prosecuted by the United States Attorney's Office for the Northern District of Illinois. In addition, a former senior Board official and current Board staff gave expert testimony at trial that led to the successful conviction.

OIG Investigations Program Receives a Clean External Peer Review Opinion

In accordance with the PCIE/ECIE *Qualitative Assessment Review Guidelines for Federal Offices of Inspector General,* the *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority,* and the PCIE/ECIE *Quality Standards for Investigations,* the PCIE/ECIE Investigations Committee determined that OIGs should undergo an independent external peer review of their investigative operations at least once every three years. The ECIE peer review process is based on these guidelines. During this reporting period, staff from the Government Printing Office (GPO) OIG conducted our first external qualitative assessment review of the investigative function. The review's overall objective was to determine whether our internal safeguards and management procedures were adequate and operating effectively to provide reasonable assurance that established policies, procedures, and applicable investigative standards were met.

In the opinion of the GPO OIG, the system of internal safeguards and management procedures of our investigative function in effect for the period ended January 10, 2008, is in compliance with the quality standards established by the PCIE/ECIE, and the guidelines issued by the Attorney General or the U.S. Marshals Service. Further, GPO OIG concluded that these safeguards and procedures provide our office with reasonable assurance of conforming to professional standards in the conduct of OIG investigations.

National Science Foundation OIG Peer Review

During the reporting period, we reviewed the system of internal safeguards and management procedures for the investigative function of the National Science Foundation OIG in effect for the period ended March 13, 2008. Our review was conducted in conformity with the above-cited applicable quality standards and related review guidelines.

Computer Forensics Examinations

We maintain a state-of-the-art computer forensics capability to ensure consistency in acquiring, handling, and examining computer media and other forms of electronic evidence in support of OIG investigations, or at the request of other law enforcement agencies. With the virtual explosion of electronic technology taking place over the last two decades, the challenge for OIG special agents to recognize and properly preserve the growing volumes of evidence stored electronically has been paramount. Evidence recoverable in criminal investigations is no longer limited to the traditional forms of computer media, such as computer hard drives or diskettes, but extends to a greater variety of easily concealable devices, including an assortment of USB removable drives, pocket drives, cellular phones, digital cameras, personal digital assistants, and similar devices. During this reporting period, in addition to supporting our own investigations, OIG special agents conducted computer forensics examinations related to two investigations at the request of another OIG.

Summary Statistics on Investigations for the Period October 1, 2007 through March 31, 2008

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	3
Investigations Open at End of Previous Period	12
Investigations Closed during Reporting Period	5
Total Investigations Active at End of Reporting Period	10
Investigative Results for this Period	
Referred to Prosecutor	1
Joint Investigations	6
Referred for Audit	0
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 117 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 whether 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 OIGs, and other financial regulatory agencies. These inquiries were referred to the appropriate Board offices, Reserve Banks, or federal and 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 fraudulent instruments that they claim are issued, endorsed, or authorized by the Federal Reserve System or a well-known financial institution.

Summary Statistics on Hotline Results for the Period of October 1, 2007, through March 31, 2008

Hotline Complaints	Number
Complaints pending from the previous reporting period	6
Complaints received during this reporting period	117
Total complaints for the Reporting Period	123
Complaints resolved during this period	114
Complaints pending	9

Legal Services

During this reporting period, the Legal Services program provided comprehensive legal advice, research, counseling, analysis, and representation in support of the OIG's projects and activities (that is, OIG audits, investigations, inspections, evaluations, and other professional, management and administrative functions). This work provides the legal basis for the conclusions, findings, and recommendations contained within OIG reports. Moreover, 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 provides selected highlights of Legal Services' work completed during this reporting period, as well as certain ongoing projects:

- Research, analysis, and legal memoranda in support of the OIG's control review of the Board's currency expenditure and assessment process, including the general legal framework surrounding the Board's currency-related activities; the legislative history of certain Federal Reserve Act provisions relating to the supervision and oversight of the currency issuance process; and the custody/ownership of currency between the Federal Reserve and BEP.
- Research of the legal requirements to conduct a Privacy Impact Assessment (PIA) on a particular Board information system.
- Processing, legal analyses, records review, responses, and coordination with the Board on Freedom of Information Act and Privacy Act requests.
- Interpretation and analysis of provisions regarding engagement letters related to the OIG's contract for the Board's financial statement audit.
- Drafting and issuance of nondisclosure agreements for contractors and peer review participants.
- Legal and historical research relating to the requirements for the Board's financial statement audits.
- Research, analysis, and advice concerning the content of OIG web pages as required by section 746 of the Consolidated Appropriations Act, 2008, Public Law 110-161.
- Legal advice and support regarding OIG personnel matters.
- Drafting and issuance of the PIA for the OIG information technology infrastructure.
- Drafting amended Privacy Act System of Records Notices for two OIG Privacy Act systems consistent with the Board-wide effort to republish the Board's entire compilation of such systems.
- Review, advice, and comments concerning various Board policies, including the Internet Use Policy and the various overtime and premium pay policies.

Our work with the OIG community continues to play an important role in the activities of the Legal Services program. OIG attorneys remained active in the Council of Counsels to the Inspector General (CCIG). We are also coordinating the government-wide OIG summer legal intern program, and are participating in the IG Academy workgroup to update and improve the legal curriculum for all

OIG law enforcement officers. We continue to help spearhead the development of a CCIG website that will serve as an aid to all OIG attorneys, and to work with the PCIE/ECIE Legislation Committee (of which the Board's IG is a member) on a variety of legislative matters potentially affecting programs and operations across the community.

In accordance with the IG Act, the Legal Services staff conducts independent reviews of newly enacted 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-four legislative and regulatory items. The following table contains selected highlights of laws and regulations that we reviewed during the reporting period:

Highlights of the OIG's Review of Laws and Regulations, October 1, 2007, through March 31, 2008

Board/Banking Legislation	
Legislation Reviewed	**Purpose/Highlights**
Money Service Business Act of 2007 (H.R. 4049)	Amends title 31 of the United States Code to eliminate burdens imposed on insured depository institutions and money services businesses, and enhances the availability of transaction accounts at depository institutions for such businesses.
Preserving and Expanding Minority Depository Institutions Act (H.R. 4043)	Amends the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 to preserve and expand minority depository institutions.
Foreclosure Prevention and Homeownership Protection Act (H.R. 3666)	Establishes a bipartisan commission, which includes the Chairman of the Federal Reserve Board, to perform a comprehensive examination of the current foreclosure and mortgage lending crisis and to make recommendations for legislative and regulatory changes to address such problems.
Openness Promotes Effectiveness in our National Government Act of 2007, or "OPEN Government Act of 2007" (S. 2488)	Amends the Freedom of Information Act by creating penalties for failure to meet timing rules, requiring specific statements of exemptions relied upon during redaction of information, and creating a new agency to administer the Act, among other things.
Federal Employees Paid Parental Leave Act of 2007 (H.R. 3799)	Amends the Family and Medical Leave Act to provide compensation to an employee for at least 8 weeks out of the 12 weeks of leave provided.
Telework Improvements Act of 2007 (H.R. 4106)	Requires each agency to establish a policy under which employees are able to telework, when authorized, for at least 20 percent of the hours worked in every two administrative workweeks.
To amend section 5112(p) of title 31, United States Code, to allow an exception from the $1 coin dispensing capability requirement for certain vending machines (H.R. 3703)	Exempts vending machines that do not accept denominations above $1 from having to dispense $1 coins as otherwise required by law.
To provide for the continued minting and issuance of certain $1 coins in 2008 (H.R. 5478)	Requires the continued minting and issuance of $1 coins that bear any design (including the Sacagawea design) until January 1, 2009.

Highlights of the OIG's Review of Laws and Regulations, October 1, 2007, through March 31, 2008 (con't)

Consumer Protection, Data Security, and Privacy Legislation	
Legislation/Regulation Reviewed	**Purpose/Highlights**
Mortgage Disclosure Improvement Act of 2007 (S. 2153 and H.R. 4019)	Amends the Truth in Lending Act to enhance disclosure of terms of mortgage loans, and for other purposes.
Mortgage Disclosure Enhancement Act of 2007 (S. 2296)	Amends the Truth in Lending Act to provide for improved disclosures by all mortgage lenders at the loan approval and settlement stages of all mortgage loans.
American Home Ownership Preservation Act of 2007 (S. 2114)	Amends the Truth in Lending Act to provide for enhanced disclosures to consumers and enhanced regulation of mortgage brokers, as well as other amendments.
Fair Disclosure for Homeowners Act of 2007 (H.R. 3705)	Amends the Truth in Lending Act to require notice to consumers of an upcoming adjustment or reset date with respect to hybrid adjustable rate mortgages.
Mortgage Kickback Preservation Act of 2007 (H.R. 3813)	Amends the Truth in Lending Act to prohibit mortgage originators from receiving any kickbacks from a mortgagor when such kickbacks are based on the terms of any residential mortgage loan.
Home Ownership Mortgage Emergency Act, or "HOME Act" (S. 2201)	Provides for the penalty-free use of retirement funds for mortgage delinquency relief.
Privacy and Cybercrime Enforcement Act of 2007 (H.R. 4175)	Amends title 18 of the United States Code to increase penalties and create new crimes relating to data privacy, and requires federal agencies to include privacy impact assessments as part of agency rulemaking under the Administrative Procedure Act.
"Prohibition on Funding of Unlawful Internet Gambling." Notice of Joint Proposed Rulemaking. (12 C.F.R. § 233) (October 4, 2007)	Implements the Unlawful Internet Gambling Enforcement Act of 2006 by providing necessary definitions, designating payment systems subject to the regulations, and providing examples of policies and procedures designed to identify and block prohibited internet gambling activity.
"Truth in Lending." Proposed Rule. (12 C.F.R. § 226) (January 9, 2008)	Amends Regulation Z by creating consumer protections for "higher-priced mortgage loans" secured by a consumer's principal dwelling, prohibiting increases in payments from creditors to mortgage brokers in violation of a consumer's agreement, and requiring clear and conspicuous mortgage loan disclosures.

Highlights of the OIG's Review of Laws and Regulations, October 1, 2007, through March 31, 2008 (con't)

Inspector General and Law Enforcement Legislation	
Legislation Reviewed	**Purpose/Highlights**
Inspector General Reform Act of 2007 (S. 2324) [H.R. 928 and S. 1723, amending the Inspector General Act, have been previously reviewed]	Amends the Inspector General Act of 1978 to enhance the effectiveness of the Inspectors General and to create a Council of the Inspectors General on Integrity and Efficiency, and for other purposes.
False Claims Act Correction Act of 2007 (S. 2041)	Seeks to amend provisions of the False Claims Act that various members of Congress believe have been incorrectly interpreted by federal courts.
National Defense Authorization Act for Fiscal Year, 2008 (H.R. 4986)	Requires all OIGs to place an annex at the end of each semiannual report describing significant audit findings in government contractor audits, and creates a Special Inspector General for Afghanistan Reconstruction.
Government Accountability Office Act of 2008 (S. 2564)	Amends the appointment process of the Comptroller General and Deputy Comptroller General at GAO and creates a statutory Office of Inspector at GAO, among other purposes.
Violent Crime Control Act of 2007 (S. 1860 and H.R. 3156)	Expands the ability of the government to prosecute for money laundering by expanding upon various definitions in title 18, United States Code, section 1956.
Court Security Improvement Act of 2007 (H.R. 660)	Amends title 18 of the United States Code to protect judges, prosecutors, federal law enforcement officers, witnesses, victims, and their family members from falsely filed liens against their property and from disclosure of restricted personal information.
Enhancing the Effective Prosecution of Child Pornography Act of 2007 (H.R. 4136)	Increases the ability of law enforcement to prosecute child pornography crimes that occur over the internet, and includes child pornography laws under "specified unlawful activity" under the money laundering statute.
Immigration Enforcement and Border Security Act of 2007 (S. 2294)	Strengthens immigration enforcement and includes criminal activity such as peonage, slavery, involuntary servitude, and harboring certain aliens under "specified unlawful activity" under the money laundering statute.
Regional Economic and Infrastructure Development Act of 2007 (H.R. 3246)	Creates five nation-wide regional development zones to increase economic development in economically distressed regions, and establishes an OIG to oversee these five regions.

Internal Operations and Community Participation

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

Internal Management Changes

The OIG enhanced our organizational structure to strengthen our ability to respond to rapidly evolving conditions in the financial markets that have a potential impact on the Board's programs and operations. By promoting senior auditors into project manager positions, we have increased our flexibility and have strengthened our succession planning framework. Building upon our matrix management approach to workflow assignments, our recent changes will help us better accomplish the goals of our Strategic Plan.

Compendium of Open Recommendations

In response to a December 2007 request from the Chairman of the House Committee on Oversight and Government Reform, we issued a *Compendium of Open Recommendations* listing those recommendations that were made during the period January 1, 2001 through January 31, 2008, and which we did not yet consider to be closed. The *Compendium* includes summary information—such as background, findings, status, and benefits that will be realized when implemented for eight reports that still had open recommendations. Where appropriate, we also noted progress that was made toward meeting each recommendation, as well as any work remaining to be done in order to close it. We did not include recommendations from OIG reports containing sensitive security issues, or information relating to OIG investigations, since our investigative reports do not contain recommendations.

Information Technology Infrastructure Enhancements

The OIG continually strives to upgrade and enhance its information technology infrastructure to more efficiently and effectively support the audit, evaluation, legal, investigative, and internal administrative functions of the office. Consistent with our information technology strategy, we recently replaced printers and are in the process of replacing laptops and servers to ensure a more reliable, compatible, and secure technology environment. We also enhanced our server clustering environment to provide a more reliable, responsive back-up and contingency capability. We have begun redesigning our publicly-available web pages to

provide greater consistency with the Board's public website, enhance our information content, and ensure compliance with applicable law. We anticipate completing the web page enhancement during the next reporting period.

Information Technology Infrastructure Certification and Accreditation

During this reporting period, the OIG completed the C&A of its information technology infrastructure as required by FISMA and the Board's Information Security Program. An independent contractor reviewed our information technology-related policies, procedures, and supporting documentation; interviewed our information technology staff; and tested selected controls. Based on this work, the contractor recommended that our infrastructure receive a full authorization to operate. We will continue to review and update our policies and procedures to incorporate the contractor's recommendations.

Executive Council on Integrity and Efficiency 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 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 also serves as an ECIE representative to the Legislation Committee, which is the central point of information regarding legislative initiatives and congressional activities that may affect the community. The IG and Assistant IG for Legal Services actively worked with staff from other OIGs and congressional committees to help ensure that pending IG Act reform legislation best reflects the needs and requirements of the IG community. OIG staff also contributed to the compilation and drafting of the recently issued PCIE/ECIE *Annual Progress Report to the President* for fiscal year 2007.

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 financial regulatory agency OIG counterparts to discuss and coordinate issues of interest, annual plans, and ongoing projects.

Committee, Workgroup, and Program Participation

The IG continues to serve on various Board committees and work groups, such as the Space Planning Executive Group and the Senior Management Council. In addition, OIG staff participate in a variety of Board working groups, including the Leading and Managing People Working Group, the Information Technology Advisory Group, the Board's Core Response Group, the Management Advisory Group, the Board's Information Security Committee, and the Board's Continuity of Operations Working Group.

Appendixes

Appendix 1
Audit Reports Issued with Questioned Costs for the Period October 1, 2007, through March 31, 2008

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, 2007, through March 31, 2008

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	03/08	1	2
Audit of Retirement Plan Administration	07/03	4	3	1	03/08	3	1
Review of the Board's Workers' Compensation Program	03/05	4	4	0	01/08	4	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	01/08	3	0
Audit of the Board's Payroll Process	12/06	7	7	0	03/08	1	6
Audit of the Board's Compliance with Overtime Requirements of the Fair Labor Standards Act	03/07	2	2	0	03/08	1	1
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	22-24
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	18
5(a)(5)/6(b)(2)	Summary of instances where information was refused	None
5(a)(6)	List of audit reports	5-9
5(a)(7)	Summary of significant reports	None
5(a)(8)	Statistical Table—Questioned Costs	31
5(a)(9)	Statistical Table—Recommendations that Funds Be Put to Better Use	32
5(a)(10)	Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made	33
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

Table of Acronyms and Abbreviations

BEP	Bureau of Engraving and Printing
Board	Board of Governors of the Federal Reserve System
BS&R	Division of Banking Supervision and Regulation
C&A	Certification and Accreditation
C&CA	Division of Consumer and Community Affairs
CCIG	Council of Counsels to the Inspector General
COS	Currency Ordering System
CRE	commercial real estate
ECIE	Executive Council on Integrity and Efficiency
FFIEC	Federal Financial Institutions Examination Council
FIRMA	Federal Reserve Integrated Records Management Architecture
FISMA	Federal Information Security Management Act of 2002
FLSA	Fair Labor Standards Act
GPO	Government Printing Office
IG Act	Inspector General Act of 1978
ISO	Information Security Officer
IT	Division of Information Technology
MGT	Management Division
NIST	National Institute of Standards and Technology
OEB	Office of Employee Benefits
OIG	Office of Inspector General
OMB	Office of Management and Budget
OSEC	Office of the Secretary
PCIE	President's Council on Integrity and Efficiency
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
SRC	Supervision, Regulation, and Credit
USB	Universal Serial Bus

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


BOARD OF GOVERNORS
OF THE FEDERAL RESERVE SYSTEM