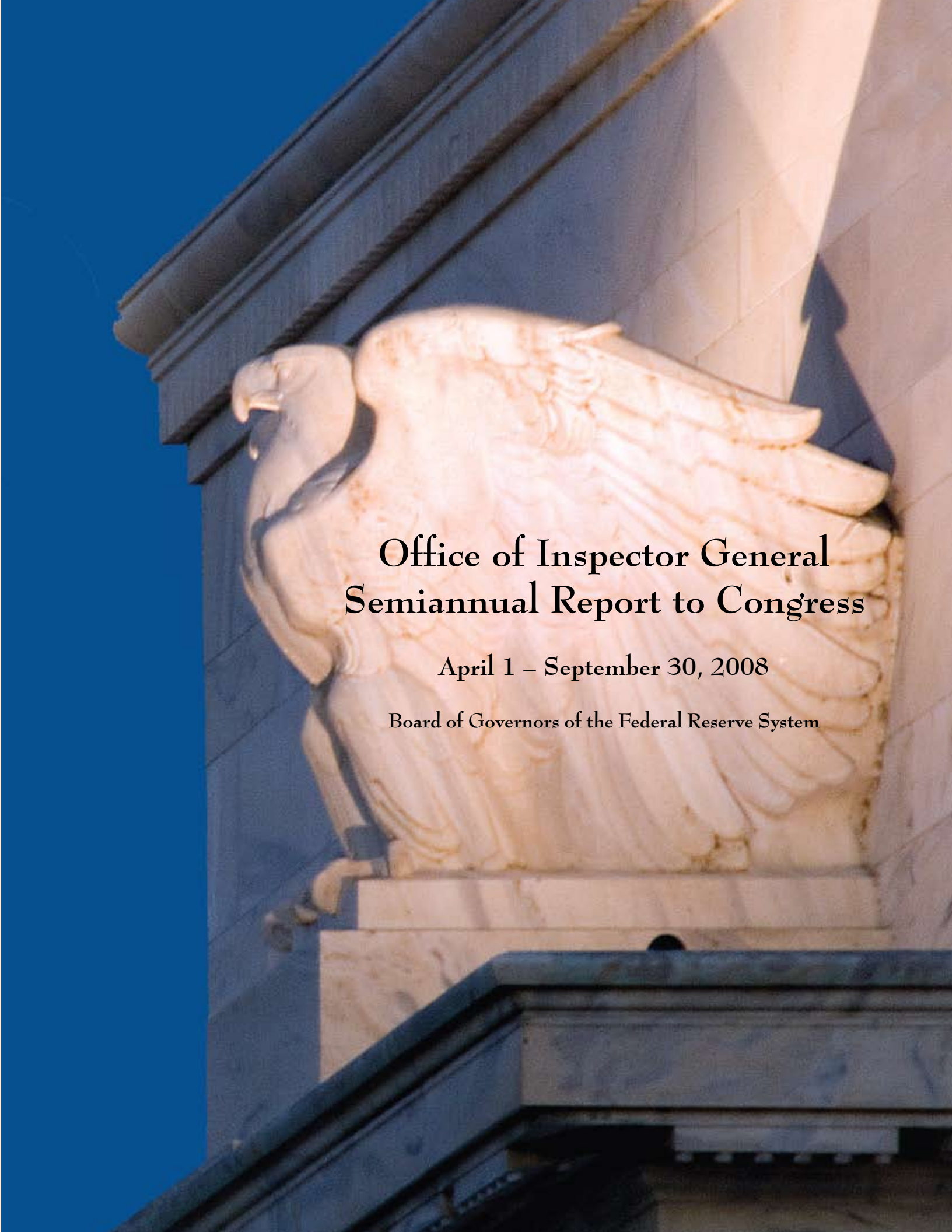


Office of Inspector General Semiannual Report to Congress

April 1 – September 30, 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

October 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 April 1 through September 30, 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

April 1 – September 30, 2008

OIG

Office of Inspector General

Table of Contents

Introduction

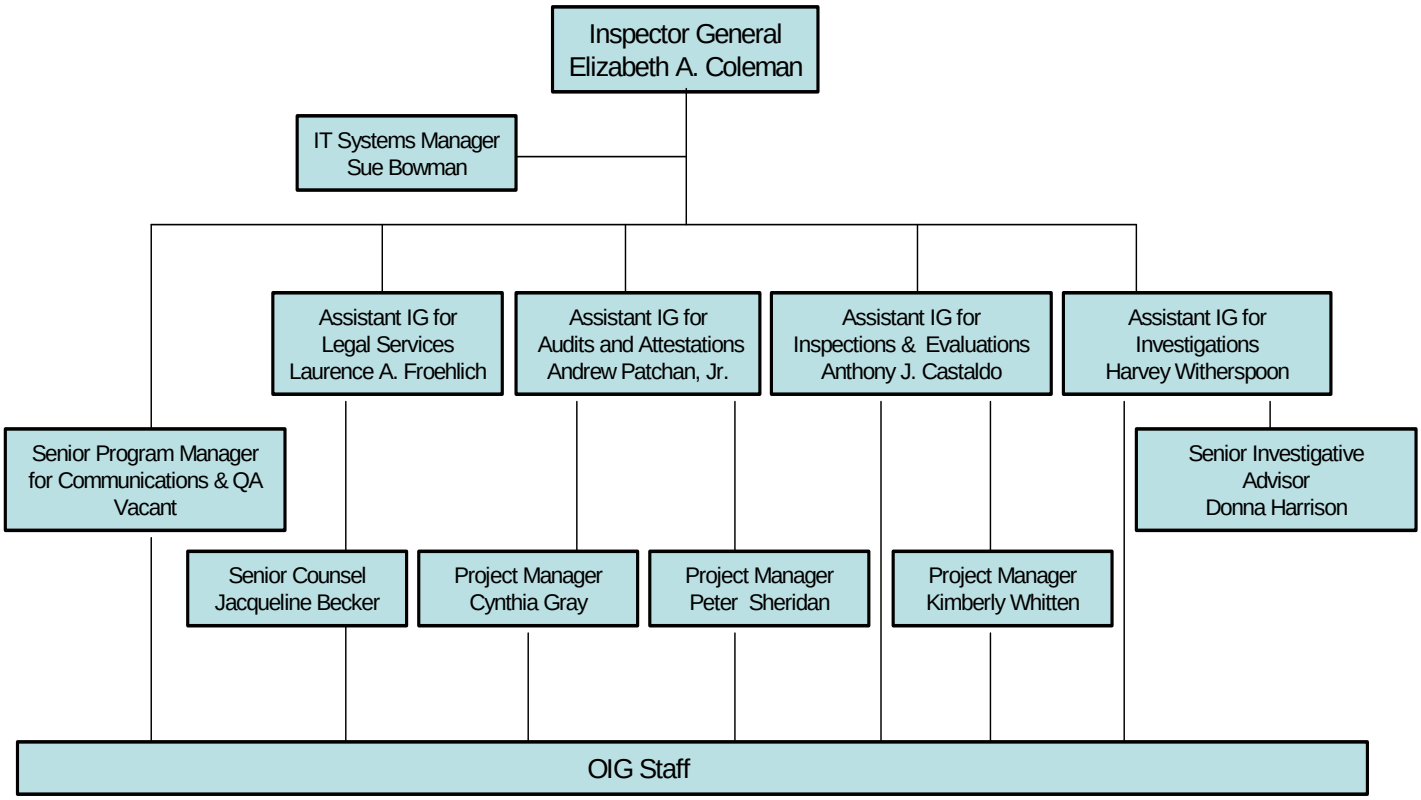
Consistent with the Inspector General Act of 1978 (IG Act), as amended, 5 U.S.C. app. 3, the mission of the Office of Inspector General (OIG) of the Board of Governors of the Federal Reserve System (Board) is to

- 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 relating to the administration of the Board's programs and operations.

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 (FDIA), 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 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 No. 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 No. 107-56, 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

October 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

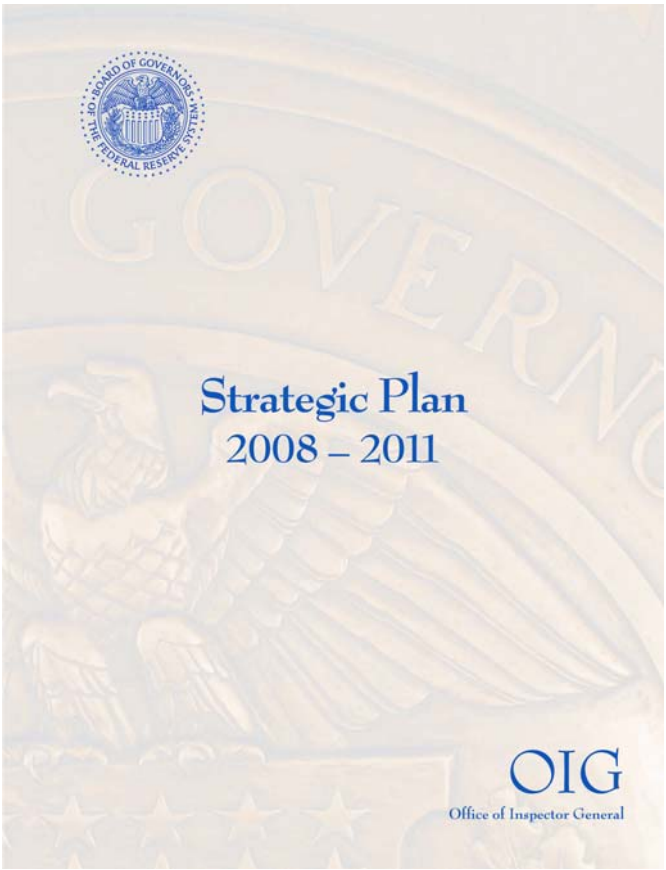
The OIG Strategic Plan establishes a results-oriented, risk-focused vision for our office, and describes the six fundamental values—independence, integrity, excellence, professionalism, empowerment, and commitment to the public interest—that shape our decisions and day-to-day operations. As indicated in the overview on page 4, we continually focus on achieving three primary goals:

(1) conduct our statutorily-mandated requirements;

(2) broaden our coverage of the Board's mission areas to enhance economy, limit risk, and detect and prevent fraud, waste, and abuse; and

(3) enhance the 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 in accordance with *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 Information Security Program

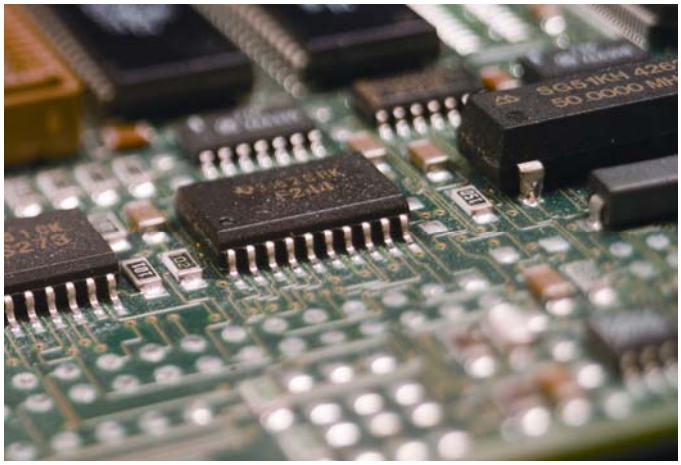
During the reporting period, we completed an audit of the Board's information security program and practices. This audit was performed pursuant to FISMA, which requires that each agency OIG conduct an annual independent evaluation of the agency's information security program and practices. Our specific audit objectives, based on the Act's requirements, were to evaluate compliance by the Board with FISMA and related information security policies, procedures, standards, and guidelines, and to evaluate the effectiveness of security controls and techniques for a subset of the Board's information systems.

To evaluate the Board's compliance with FISMA and related policies and procedures, we reviewed components of the Board's certification and accreditation (C&A) process, including risk assessments, security plans, and security assessments. We also collected and reviewed information concerning the Board's processes related to areas for which the Office of Management and Budget requests a specific response as part of the agency's annual FISMA reporting. Our work included analyzing the Board's security-related processes for security awareness and training, remedial action monitoring, incident response, configuration management, controls over personally identifiable information (PII), and privacy impact assessments.

Overall, we found that the Board continues to advance and improve its information security program. During 2008, the Board enhanced its annual security awareness training and its processes for tracking security-related issues and initiatives. It also certified and accredited minor applications and subsystems by bundling them (1) under the security plans of a General Support System (GSS) or a major application that provides a significant portion of its security control requirements; or (2) with other minor applications to form a single major application. We found that the Board's inventory has remained stable since 2007,

and that the bundling of minor applications and subsystems is a reasonable approach to implement the Board's security program.

However, our review of the C&A of major applications and the central GSS supported by the Division of Information Technology (IT) identified opportunities for the Board to improve its risk assessment process and security assessment testing. We found that the risk assessments can be improved to explicitly identify the residual risk remaining, and the additional security controls needed, after implementing minimum baseline controls. We also found that the security assessments performed as part of the C&A process need to be strengthened to include necessary and sufficient independent testing to provide the system owners with assurance that information security controls for these systems are effectively implemented and functioning as intended. Our report contained two recommendations to the Chief Information Officer (CIO) designed to ensure that (1) risk assessments adequately identify, evaluate, and document the level of risk to an information system based on potential threats, vulnerabilities, and currently implemented or planned controls to determine if additional controls are needed; and (2) security assessments include necessary and sufficient independent testing to support the authorization for the system to operate, and to provide the authorizing official and the Board assurances that information security controls for these systems are implemented correctly, working as intended, and producing the desired results.



We provided our draft report for review and comment to the Director of IT, in her capacity as the CIO for FISMA. The director concurred with our recommendations.

Information Security Control Reviews

To evaluate security controls and techniques for a subset of the Board's information systems, we review controls over Board applications on an ongoing basis. During this period, we completed security control reviews of the Currency Ordering System (COS) and two third-party applications supported by the Federal Reserve Bank of Boston (FRB Boston) in support of the Board's supervision and regulation function.

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, *Recommended Security Controls for Federal Information Systems*. This document provides a baseline for managerial, operational, 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, which were restricted given the sensitivity of the issues involved with these reviews. We provided the specific results to the appropriate division directors in separate restricted reports, for review and comment, each of which is summarized below.

Security Control Review of the Currency Ordering System

COS is listed as a major application on the Board's FISMA application inventory for the Division of Reserve Bank Operations and Payment Systems (RBOPS), and it includes two subsystems: Carrier Billing Online (CBO) and Special Shipments. These subsystems share a common operating environment, but perform different functions. Specifically, COS enables users from the Board, the Bureau of Engraving and Printing (BEP) of the U.S. Department of the Treasury, and the Federal Reserve Banks to monitor and control the production, inventory, and distribution of new currency throughout the United States. CBO is designed to 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. Special Shipments is designed to maintain and track shipments that are transported from one Federal Reserve Bank to another.

Overall, COS and its subsystems generally met control objectives for four of the ten families we reviewed, and nothing came to our attention regarding deficiencies in the design or implementation of the controls for these families. However, our testing did not include all controls within every family, and our fieldwork was based on information available at the time of our review. For those control families where control objectives were not met, we identified the aspect of the control that needs improvement, is missing, or is deficient, and highlighted the recommended action. The Director of RBOPS generally agreed with our recommendations and indicated that corrective action has either been taken or is under way to enhance the specific controls highlighted in the report.

Security Control Reviews of Two Federal Reserve Bank of Boston Applications

FRB Boston maintains two systems that have been classified as a GSS and a major third-party application, respectively, on the Board's FISMA application inventory for the Division of Banking Supervision and Regulation (BS&R): the Supervision and Regulation (S&R) Infrastructure, and Notes Applications. The S&R Infrastructure consists of various hardware and software components configured to provide information technology tools and support for FRB Boston's Supervision, Regulation, and Credit Group operations. The Notes Applications is a bundle of two database applications used to support bank examinations.

Overall, the S&R Infrastructure and Notes Applications generally met control objectives for nine of the seventeen families we reviewed, and nothing came to our attention regarding deficiencies in the design or implementation of the controls for these families. However, our testing did not include all controls within every family, and our fieldwork was based on information available at the time of our review. For those control families where control objectives were not met, we identified the aspect of the control that needs improvement and highlighted the recommended action. The Directors of BS&R and IT generally agreed with our recommendations and indicated that corrective action has either been taken or is under way to enhance the specific controls highlighted in the report.

Currency Expenditure and Assessment Control Review

The Federal Reserve Act (Act) establishes broad authorities and responsibilities related to the production, distribution, and destruction of Federal Reserve notes. For example, the Act authorizes the Board to issue notes at its discretion and provides that such notes are obligations of the United States. The Act also authorizes the Board to levy an assessment on the Federal Reserve Banks to pay for all expenses related to producing, issuing, and retiring Federal Reserve notes. The Board prepares and submits to the BEP an annual order for new currency production, and contracts with commercial armored carriers to deliver the new currency to the Federal Reserve Banks and branches, and within the Federal Reserve System. Ensuring that sufficient currency is in circulation to meet public demand is an important responsibility of the Federal Reserve System, and the expenses associated with this function are the largest line item on the Board's annual financial statements, totaling approximately $576 million in 2007.

Our objective was to evaluate the effectiveness of the Board's controls over processes to record currency expenses and to levy assessments on the Reserve Banks for these expenses. More specifically, we assessed whether the controls over these transactions are designed and operate effectively to provide reasonable assurance that records and transactions are maintained in sufficient and accurate detail; financial transactions are processed in compliance with applicable laws, regulations, and management's authorization; and unauthorized or fraudulent transactions are prevented or can be detected in a timely manner. As part of our review, we developed detailed flowcharts and narratives of the Board's expenditure and assessment processes for each currency expense, including the Board's interaction with BEP for currency production and billing. We used the flowcharts to identify controls, and tested certain controls by tracing currency-related transactions through the Board's expenditure and assessment processes.

Overall, we found that the Board has controls over the processes to record currency expenses and to levy assessments on the Reserve Banks for these expenses, and that the majority of the controls were operating effectively. We did not detect any instances of fraud or other improprieties. Although our testing did not identify any significant discrepancies, we did find opportunities to strengthen

the Board's controls for paying currency invoices, preparing and processing assessments, monitoring vendor performance, and reporting the currency expenses in the Board's financial statements. In addition, fully implementing certain automated controls in the Board's financial management system would improve controls and reduce manual processing. Finally, while we found that the Board has a good working relationship with BEP and has established compensating controls and processes related to printing expenses, we believe that the Board should strengthen the current inter-agency agreement with BEP by formalizing existing operational reviews and enhancing inventory controls. Our report contains six recommendations designed to address these issues and help maintain an effective system of internal controls.

We provided a copy of our report to the Directors of the Management Division and the Division of Reserve Bank Operations for review and comment. In their joint response, the directors agreed with the report recommendations and discussed actions already underway or that will be taken to implement the recommendations.

External Peer Review of the OIG

Generally Accepted Government Auditing Standards (GAGAS) require organizations performing audits in accordance with these standards to undergo an external peer review of their auditing practices at least once every three years. The overall objective of the review is to determine whether the OIG's internal quality control system is adequate as designed and provides reasonable assurance that the OIG followed applicable auditing standards, policies, and procedures. The peer reviews are conducted in accordance with standards and guidelines established by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).

During this reporting period, staff from the Government Printing Office (GPO) OIG reviewed our audit operations. In the opinion of the GPO OIG, the system of quality control for our audit function was designed in accordance with the quality standards established by the PCIE and ECIE. Further, our audit function was in compliance with the quality control system for the eighteen-month period ending March 31, 2008, and provides the OIG with reasonable assurance of material compliance with professional auditing standards in the conduct of our audits. Therefore, the GPO OIG issued an unmodified opinion on our system of audit quality control.

FOLLOW-UP ACTIVITIES

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

During the reporting period, we completed a second follow-up to our May 2005 *Report on the Audit of the Board's Fixed Asset Management.* That report contained two recommendations designed to address fixed asset management issues related to policies, financial system usage, and internal controls. Our initial follow-up, completed in March 2006, determined that the Board issued a new property management policy that incorporates accounting-related policies and procedures; therefore, we closed that recommendation. However, because other corrective actions had not been fully implemented by MGT, the recommendation related to improving financial system usage and internal controls was kept open.

During our second follow-up, we met with Board management and staff, reviewed pertinent documents, and tested fixed assets purchased subsequent to the issuance of the new policy and the implementation of revised asset management procedures. We found that MGT has implemented additional functionality within the Board's financial system, developed a new "Capital Purchase Information Form" and modified procedures for ensuring that sufficient descriptive information is recorded for each asset, and established separation of duties between the property management and accounting function. These actions were sufficient to close the second recommendation.

Follow-up of the Audit of the Federal Reserve's Background Investigation Process

Our October 2001 report contained three recommendations designed to enhance the background investigations process for employees and other individuals who access Board premises regularly, such as contractors and temporary employees. We had already closed the first recommendation that called for updating and clarifying background investigation policies and procedures, and have now completed further analysis and testing for the remaining two recommendations. We determined that the Board's actions to issue guidance, policies, and procedures for conducting background investigations on contractors, summer interns, temporary employees, and transferred employees were sufficient to close the other two recommendations.

ONGOING AUDIT WORK

Security Control Review of the Electronic Security System

During this period, we began a security control review of the Electronic Security System (ESS). ESS is listed as a major application on the Board's FISMA

application inventory for MGT. ESS augments the Board's physical security by providing one uniform system for badge issuance and access control, as well as for closed-circuit video surveillance, capture, and playback. The objective of our review is to evaluate the adequacy of control techniques for protecting the system's data from unauthorized access, modification, destruction, or disclosure. We expect to finish our control testing and present our results to management in the next reporting period.

Audit of Infrastructure Audit Logging

We began an audit of audit logging across the IT-supported, central GSS (the IT GSS) as part of our ongoing evaluation of the Board's compliance with its information security policies and procedures. Our objectives are to identify the manner in which audit logging is performed across the IT GSS, review events being logged in the IT GSS, and validate that security controls have been implemented and tested as part of the C&A of the IT GSS. We expect to complete this project and issue our final report in the next reporting period.

Management and Accountability of Mobile Computing Devices

We continued our audit of the management and accountability of mobile computing devices used by the Board. We began 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, the protection of 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 Universal Serial Bus (USB) flash drives. During this reporting period, we completed testing of the process controls, including key controls. We anticipate discussing our results with management and issuing our final report in the next reporting period.

Audit of Internal Controls over Board Cell Phones

We began an audit of the internal controls over Board cell phones and smart phones to evaluate the effectiveness of the Board's recently revised cell phone and smart phone procedures. Specifically, we are evaluating the controls over the receipt, tracking, securing, and disposal of cell phones and smart phones. To accomplish our objective, we are conducting interviews, developing process flowcharts, and testing key controls to determine if controls are working as intended.

Audit of the Board's Transportation Subsidy Program

We began an audit of the Board's transportation subsidy program to evaluate whether the program is properly controlled and efficiently administered. Specifically, we are assessing the extent to which existing internal controls (1) ensure compliance with applicable laws and regulations and management's authorization, and (2) prevent unauthorized or fraudulent activities. During this reporting period, we interviewed Board staff, identified key process controls, developed process flow charts, and devised a risk control matrix. We plan to test controls during the next reporting period and will present our results to management once testing is completed.

The SmarTrip logo is the registered service mark of WMATA. WMATA approved the use of this logo.

Audit of the Board's Financial Statements for the Year Ending December 31, 2008, and Audit of the Federal Financial Institutions Examination Council's Financial Statements for the Year Ending December 31, 2008

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). [Note: The Board performs the accounting function for the FFIEC.] Deloitte & Touche LLP, our contract auditors, perform the audits to obtain reasonable assurance about whether the financial statements are free of material misstatement. The audits include examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. The audits also include an assessment of the accounting principles used, and significant estimates made, by management, as well as an evaluation of overall financial statement presentation.

To determine the auditing procedures needed to express an opinion on the financial statements, the auditors will consider the Board's and the FFIEC's internal controls over financial reporting. As part of obtaining reasonable assurance about whether the financial statements are free of material misstatement, the auditors also will perform tests of the Board's and the FFIEC's compliance with certain provisions of laws and regulations, since noncompliance with these provision could have a direct and material effect on the determination of the financial statement amounts. We anticipate receiving the external auditor's report in the next reporting period.

Smithsonian Institution OIG Peer Review

We reviewed the system of quality control for the audit function of the Smithsonian Institution (SI) OIG in effect for the fourteen month period ending May 31, 2008. GAGAS requires government audit organizations to undergo periodic external peer reviews at least once every three years in order to determine whether the organization's internal quality control system is adequate as designed and complied with, and to provide reasonable assurance that applicable auditing standards, policies, and procedures have been met. A system of quality control covers an OIG's organizational structure, and the policies adopted and procedures established to provide it with reasonable assurance of conforming with GAGAS. Our review was conducted in accordance with standards and guidelines established by the PCIE and the ECIE. A discussion draft report was provided to the SI Inspector General, and we anticipate issuing a final report 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 extensive 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 PCIE and ECIE.

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

During this period, we completed an evaluation of the controls over data flowing from the Board to the Office of Employee Benefits (OEB) and its contractors. We initiated this evaluation after our office and the Board's external auditor identified discrepancies in employee benefits-related data between the Board's information system and the system maintained by an OEB contractor that serves as the record keeper for the Federal Reserve System's Retirement, Thrift, Long-Term Disability, and Supplemental Survivor Income plans. Our objective was to determine the adequacy and effectiveness of controls over Board employee information that is received, processed, and disseminated by OEB and its contractors.

Overall, our analysis and testing revealed that, in most instances, controls over the flow of Board employee data were adequate to ensure that the data was accurately received and processed by OEB and its contractors. We did, however, make two recommendations to (1) eliminate the potential for errors in part-time employees' retirement benefit calculations, and (2) automate certain manual steps that Board employees must take to process and send employee data to an OEB contractor. We presented our results (restricted because they contain details on information security-related internal controls) to MGT staff and to the Committee on Plan Administration, and received concurrence on both recommendations.

Reducing the Risk of Loss or Theft of Confidential Information: Comparison of Agencies' Requirements

Highly publicized incidents have drawn attention to the risks associated with the theft or loss of confidential information, including PII. In response, OMB issued guidance outlining agencies' responsibilities for safeguarding and protecting sensitive information that is processed on computers and related hardware.

In light of the enhanced government-wide attention on securing PII, the Staff Director for Management (Staff Director) expressed interest in an analysis of steps that other agencies were taking to mitigate 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' processes, we performed an evaluation that involved compiling policies, procedures, and requirements for safeguarding electronic devices and confidential information for nine federal agencies, including four federal financial regulators. We then compared the other agencies' requirements to the Board's policies and procedures that address handling PII and other sensitive or confidential information.

We discussed the results of our evaluation (restricted because of the sensitivity associated with work related to safeguarding confidential information) during a briefing to the Staff Director and the Director of IT. Overall, we found that the Board's policies address almost all of the other agencies' requirements for reducing the risk of theft or loss of confidential information while employees are traveling or working outside of their offices. Nevertheless, we made several suggestions to the Staff Director that we believe will further enhance the effectiveness of the Board's policies. In addition, we commended the Board's plans to develop a web page to build awareness of privacy issues, and suggested that the web page provide a central source of information and guidance that integrates Board policies, procedures, and practices related to safeguarding confidential information and PII.

Evaluation of Certification and Accreditation Reviews of the National Examination Database

Concurrent with audit work performed pursuant to the requirements of FISMA, we conducted an evaluation that focused on the Board's C&A reviews of the National Examination Database (NED) to help us gain a perspective on the evolving C&A process. Our objective was to assess the Board's progress as it conducted C&A reviews in accordance with guidance issued by the NIST and the Board. The evaluation focused on the depth, scope, and completeness of the C&A reviews performed and the sufficiency of information that the NED system owner and authorizing official had available to make their accreditation decision.

As noted in a management letter to the Director of IT, our NED evaluation observations were consistent with our 2008 information security program audit report's conclusion that security assessments, performed as part of the C&A process, need to be strengthened to include sufficient independent testing to provide system owners with assurance that information security controls are effectively implemented and operating as intended.

ONGOING INSPECTIONS AND EVALUATIONS

Maintaining Readiness to Perform a Material Loss Review

The FDIA, as amended, requires that the Inspector General of the appropriate federal banking agency review the agency's supervision of a failed institution when the projected loss to the Deposit Insurance Fund is considered material. In addition, the cognizant Inspector General is required to produce, within six months of the loss, a report that includes possible suggestions for improvement in the agency's banking supervision practices. According to the FDIA, a loss is material if it exceeds the greater of $25 million or two percent of the failed institution's total assets. The Federal Reserve is the primary supervisor for state member banks, and our office would review any failed state member bank that exceeds the materiality threshold.

From January 1, 2008, to September 30, 2008, thirteen insured financial institutions failed. The Federal Deposit Insurance Corporation (FDIC) projects that the losses incurred by eight of these institutions meet the material loss threshold and, therefore, require an Inspector General to perform a material loss review (MLR). As of October 2008, however, none of these failed institutions have been state member banks. Nevertheless, the current economic and banking climate heightens the potential for a state member bank failure that may trigger a MLR.

We are working closely with the other federal financial regulatory Inspectors General to monitor the condition of troubled institutions. Moreover, we are maintaining our readiness to perform a MLR by analyzing banking industry trends and reports generated by the Board's BS&R Division, refining our MLR methodology, and ensuring that staff receive on-the-job and external training in a variety of banking topics.

Inspection of the Board's Law Enforcement Unit

The USA PATRIOT Act of 2001 granted the Board certain federal law enforcement authorities, and the regulations implementing this new authority—*Uniform Regulations for Federal Reserve Law Enforcement Officers*—designated the OIG as the External Oversight Function (EOF). We have initiated an inspection of the Law Enforcement Unit (LEU) to continue fulfilling our EOF responsibility for conducting a continuous review of Board law enforcement programs and operations. We have identified areas that pose the highest risks to the LEU's operations and will focus our inspection fieldwork on evaluating the effectiveness of controls designed to mitigate these risks. In addition, we will evaluate the LEU's compliance with applicable laws, regulations, and Board policies.

Investigations

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

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

Alleged Conflict of Interest by a Former FRB Richmond Employee

During the current reporting period, the OIG completed a joint investigation with the Charlotte Division of the Federal Bureau of Investigation and the United States Attorney's Office for the Western District of North Carolina regarding an alleged conflict of interest by a former Assistant Examiner with the Federal Reserve Bank of Richmond's Charlotte Office. This investigation was initiated after the FBI and OIG received information that the examiner may have negotiated for future employment with a state member bank while he was participating in an examination of that bank. We found that the examiner submitted his resume to the state member bank five days before he was assigned to a key position with the responsibility to conduct a targeted on-site examination of that bank. In addition, we found that during the on-site phase of the examination, the examiner met with the bank's staff to discuss prospective employment. Prosecution was declined because the investigation did not disclose any evidence that the examiner either used his position to influence the examination process in order to further his own financial interest, or was involved in a *quid pro quo* arrangement with the state member bank.

Alleged Misuse of the Government Travel Card

During this reporting period, we 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 repeatedly misused the GTC, after receiving three warnings for using the GTC inappropriately for cash advances in the New York and Philadelphia, Pennsylvania areas to pay for gambling activities at various casinos in Atlantic City, New Jersey. In addition, as of April 2008, the outstanding balance on the employee's GTC account was about $10,700 and was nearly 120 days delinquent. The investigation confirmed that, after receiving the three warnings, the employee obtained numerous unauthorized cash withdrawals for personal use at gambling

casinos. The investigation also confirmed that the employee had received reimbursement for all official travel related expenses and that his delinquent account was for nonpayment, and not the result of either a dispute with the credit card company or a delay on the Board's part for not reimbursing the employee. The employee was suspended for fourteen calendar days, without pay.

ONGOING INVESTIGATIVE ACTIVITIES

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 ongoing criminal investigative activity involved leading or participating in a number of multi-agency task forces where alleged bank fraud, terrorist financing, and money laundering were among the crimes that are 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. Due to the sensitivity of these investigations, we only report on concluded activities referred for prosecutorial or administrative action.

Summary Statistics on Investigations for the Period April 1, 2008, through September 30, 2008

Investigative Actions	Number
Investigative Caseload	
Investigations Opened during Reporting Period	2
Investigations Open at End of Previous Period	10
Investigations Closed during Reporting Period	4
Total Investigations Active at End of Reporting Period	8
Investigative Results for this Period	
Referred to Prosecutor	0
Joint Investigations	3
Referred for Audit	0
Referred for Administrative Action	1
Oral and/or Written Reprimand	0
Terminations of Employment	0
Arrests	0
Suspensions	1
Debarments	0
Indictments	0
Convictions	0
Monetary Recoveries	$0
Civil Actions (Fines and Restitution)	$0
Criminal Fines: Fines & Restitution	$0

Hotline Operations

The OIG received 264 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. Examples of these schemes are the highly publicized Nigerian e-mail scams and other similarly fraudulent activities.

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

Summary Statistics on Hotline Results for the Period of April 1, 2008, through September 30, 2008

Hotline Complaints	Number
Complaints pending from the previous reporting period	9
Complaints received during this reporting period	264
Total complaints for the Reporting Period	273
Complaints resolved during this period	266
Complaints pending	7

Legal Services

The Legal Services program provides comprehensive legal advice, research, counseling, analysis, and representation in support of 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 the OIG staff aware of recent legal developments that may affect the activities of the OIG and the Board.

The following illustrates selected highlights of Legal Services' work completed during this reporting period:

- tracking, analysis, and negotiation of legislative proposals to significantly amend the IG Act
- professional training sessions provided to OIG staff concerning: the Board's actions related to the Bear Stearns collapse; the Board's enforcement program as carried out by the BS&R; and legal aspects of the Right to Financial Privacy Act
- analysis and negotiation of terms pertaining to certain OIG software licensing agreements
- analysis of legal requirements to report computer security incidents to USCERT
- processing Freedom of Information Act (FOIA) and Privacy Act requests, including legal analyses, records review, responses, and coordination with the Board
- review of requests for IG administrative subpoenas for legal justification, recommendation for issuance, and processing
- interpretation and analysis of provisions regarding engagement letters under the OIG's contract for the Board's financial statement audit
- negotiation of a memorandum of understanding between the Board's OIG and the SI OIG concerning our peer review of the SI OIG
- compilation of legislative history and other legal research relating to OIG requirements to comply with GAGAS
- research and advice concerning the content of the OIG web site
- advice and support for OIG human resource and personnel matters
- interpretation of FOIA definition of "agency record," and applicability of exemptions to certain Board and OIG information

The legal staff is also involved in a variety of ongoing projects, including researching and analyzing the Board's policy on protecting PII, and the laws related to the Board's transportation subsidy program. In addition, the Legal staff has reviewed the recently-enacted Emergency Economic Stabilization Act of 2008 (Pub. L. No. 110-343, October 3, 2008) and is analyzing the legislation to determine its likely impact on Board programs and operations, and to facilitate planning for OIG work in areas affected by the new law.

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. Legal services also coordinates OIG comments on proposed Board policies. During this reporting period, Legal Services reviewed twenty-eight legislative and regulatory items. Among the regulations and Board policies reviewed were the Board's:

- Notice of Proposed Rulemaking to amend Regulation S
- draft Notice of Proposed Rulemaking to amend "Capital Treatment Rules for Goodwill Arising from a Taxable Business Combination"
- draft revised Transportation Subsidy Policy
- "Policy for Handling Personally Identifiable Information"
- updated "Data-Breach-Notification Policy and Plan"

The following table contains selected highlights of legislative items that we reviewed during the reporting period.

Highlights of the OIG's Review of Existing and Proposed Legislation, April 1 through September 30, 2008

Board/Banking Legislation	
Legislation Reviewed	**Purpose/Highlights**
Plain Language in Government Communications Act of 2007 (S. 2291 and H.R. 3548)	Requires all federal agencies to use plain language when information is provided to the public about government requirements, programs, benefits, and services; agencies must report to Congress on progress and appoint a senior officer in charge of compliance.
Price Stability and Inflation Targeting Act of 2008 (H.R. 6042)	Establishes price stability as the primary goal of monetary policy of the Board and the Federal Open Market Committee.
Price Stability Act of 2008 (H.R. 6053)	Requires the Board to establish an explicit numerical definition of the term "price stability" and maintain a monetary policy that promotes long-term price stability.
Sound Dollar and Economic Stimulus Act of 2008 (H.R. 6690)	Requires the Board to maintain the U.S. dollar at a price of the market value of 0.05 of a troy ounce of gold.
To prohibit the Board of Governors of the Federal Reserve System from making funds available at a discount rate to private individuals, partnerships, and corporations (S. 3510)	Amends the Federal Reserve Act to repeal section 13(3), thereby preventing the Board from making funds available at a discount to private individuals, partnerships, and corporations.
Coin Modernization and Taxpayer Savings Act of 2008 (H.R. 5512)	Establishes composition restrictions on the 1-cent and 5-cent coins and, alternatively, permits the Secretary of the Treasury to research new and cheaper coin compositions.
Family Fairness Act of 2008 (H.R. 6029)	Extends the benefits of the Family and Medical Leave Act to part-time employees who have worked for an employer for at least 12 months.
Regulatory Relief and Fairness Act (S. 2703 and H.R. 1550)	Requires the SEC to issue regulations to allow an insured depository institution, a bank holding company, and a savings and loan holding company to elect not to provide a certification or an internal control report, as otherwise required under the Sarbanes-Oxley Act of 2002.
Emergency Economic Stabilization Act of 2008 (H.R. 1424, became Pub. L. No. 110-343, October 3, 2008)	Provides authority for the federal government to purchase certain types of troubled assets for the purposes of providing stability or preventing disruption to the financial markets or banking system, establishes various Board-related responsibilities.

Highlights of the OIG's Review of Existing and Proposed Legislation, April 1 through September 30, 2008—*Continued*

Inspector General and Law Enforcement Legislation	
Legislation Reviewed	**Purpose/Highlights**
Emmett Till Unresolved Civil Rights Crime Act of 2007 (H.R. 923, became Pub. L. No. 110-344, October 7, 2008)	Authorizes all Inspectors General to assist the National Center for Missing and Exploited Children by conducting reviews of inactive case files to develop recommendations for further investigations.
Government Credit Card Abuse Prevention Act of 2007 (S. 789 and H.R. 1395)	Requires the head of each executive agency to establish various safeguards and controls relating to purchase cards, travel cards, and centrally-billed accounts; requires OIG review of such controls.
Housing and Economic Recovery Act of 2008 (H.R. 3221, became Pub. L. No. 110-289, July 30, 2008)	Creates a new independent federal agency known as the Federal Housing Finance Agency, with a new Office of Inspector General, and abolishes the current agencies of the Office of Federal Housing Enterprise Oversight and the Federal Housing Finance Board.
Government Accountability Office (GAO) Act of 2008 (H.R. 5683, became Pub. L. No. 110-323, September 22, 2008)	Requires executive agencies to reimburse GAO for the cost of certain financial statement audits.
Government Accountability Office Improvement Act of 2008 (H.R. 6388)	In order to repudiate a district court decision, restores GAO's authority to pursue litigation if an agency improperly withholds records from GAO; and establishes the federal courts as a forum for enforcing GAO's right to access such information.
Close the Contractor Fraud Loophole Act (H.R. 5712)	Mandates timely notification by federal contractors of violations of federal criminal law or overpayments in connection with the award or performance of contracts or subcontracts.
Incorporation Transparency and Law Enforcement Assistance Act (S. 2956)	Subjects persons, who act on behalf of another to assist in formation of a corporation, to federal anti-money laundering laws; requires states to track the "beneficial owners" of corporations and limited liability companies.
Intelligence Authorization Act for Fiscal Year 2009 (S. 2996)	Amends the National Security Act of 1947 to clarify the duties and responsibilities of the Inspector General of the Intelligence Community.
To elevate the Inspector General of the Commodity Futures Trading Commission to a presidentially-appointed Inspector General, in accordance with section 3 of the Inspector General Act of 1978 (H.R. 6406)	Amends the Inspector General Act of 1978 in order to make the Inspector General of the Commodity Futures Trading Commission a presidentially-appointed Inspector General.

Highlights of the OIG's Review of Existing and Proposed Legislation, April 1 through September 30, 2008—*Continued*

Consumer Protection, Data Security, and Privacy Legislation	
Legislation Reviewed	**Purpose/Highlights**
Protecting Consumers from Unreasonable Credit Rates Act of 2008 (S. 3287)	Establishes a national usury rate of 36 percent which cannot be exceeded in a consumer credit transaction; provides for civil and criminal liability.
Over-Classification Reduction Act (H.R. 6575)	Requires the Archivist of the United States to promulgate regulations to prevent the over-classification of government information; requires Inspectors General to conduct random audits of their agency's information classification procedures.
Reducing Information Control Designations Act (H.R. 6576)	Limits the ability of federal agencies to withhold information by designating it as "sensitive but unclassified" or "for official use only;" and requires the Inspector General of each federal agency to audit information classification procedures to ensure compliance with this legislation.
Federal Information Security Management Act of 2008 (S. 3474)	Amends the current Federal Information Security Management Act to require IGs to perform an annual "audit" rather than an "evaluation;" creates the position of a "Chief Information Security Officer" and establishes a "Chief Information Security Officer Council;" and establishes reporting requirements for agency heads and IGs.

OIG Operations and Community Participation

While the OIG's primary mission is to enhance Board programs and operations, we also work internally and coordinate externally to achieve our goals and objectives. Internally, we consistently strive to enhance and maximize efficiency in our infrastructure and day-to-day operations. Within the Board and the Federal Reserve System, we continue to provide information about the OIG's roles and responsibilities. Externally, we are active members of the broader IG and professional communities and we promote coordination on shared concerns. Highlights of our activities follow:

Information Technology Infrastructure Enhancements

During this reporting period, we continued to upgrade and enhance our IT infrastructure to more efficiently and effectively support the audit, evaluation, legal, investigative, and internal administrative functions of the office. We have moved our public web pages to the Board's public web site to ensure compliance with applicable laws. Through coordination with the Board's public web team, the OIG made substantial progress in redesigning publicly-available web pages, and plans to roll them out during the next reporting period. The OIG also continues to update and strengthen the OIG Continuity of Operations Plan to ensure the performance of the OIG's critical functions during emergency events.

Recommendation Follow-up System

The OIG is in the process of implementing an automated follow-up and tracking system that will provide both OIG auditors and Board staff with an interactive platform to document and collaboratively assess progress made in responding to OIG recommendations. We are currently testing the software's functionality and security. During the next reporting period, we plan to pilot test the system with staff from the IT Division and, subsequently, begin a Board-wide roll-out.

Financial Regulatory OIG Coordination

To foster collaboration and cooperation on issues of mutual interest, including issues related to the current financial crisis, the Board's IG meets regularly with the IGs from other federal financial regulatory agencies: the FDIC, 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 [soon to be subsumed by the Federal Housing Finance Agency]. In addition, 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, including bank failure MLR best practices, annual plans, and ongoing projects.

Executive Council on Integrity and Efficiency Participation

The Board's IG serves as a member of the ECIE, which was created by Executive Order 12805 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 have actively and successfully worked and negotiated with staff from other OIGs and congressional committees to ensure that the IG Act reform legislation—Inspector General Reform Act of 2008, Public Law No. 110-409, October 14, 2008—best reflects the needs and requirements of the IG community. Among other changes for the IG community, in early 2009, the ECIE and PCIE will be replaced by a single, statutory council of all Inspectors General.

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. Externally, OIG Legal Staff are members of the Council of Counsels to the Inspector General (CCIG). They are also active members of the CCIG web site development team, and were very involved with the OIG Credentials Language Working Group that drafted model language for use government-wide by the various Inspector General offices. In addition, the Assistant IG for Audits and Attestations serves as Co-Chair of the IT Committee of the Federal Audit Executive Council, and works with audit staff throughout the IG community on common IT audit issues.

Professional Development Activities

For the third consecutive year, OIG Legal staff have coordinated the government-wide OIG summer legal intern program. This program offers law students exposure to the wide range of legal services performed by IG Counsels, as well as an introduction to the practice of law, generally, in the federal government. The law interns get an opportunity to network across agencies, as well as to speak with various Inspectors General, Department of Justice attorneys, and lawyers in the Legislative and Judicial branches. Legal staff also participated in the IG Academy workgroup to update and improve the legal curriculum for all OIG

federal law enforcement officers. Working with other IG counsels, the OIG Legal staff helped to develop and present a legal refresher training program for OIG investigators from agencies across the government. This training program focuses on civil and administrative investigations, and will become part of the Federal Law Enforcement Training Center curriculum. OIG Legal staff also developed and presented three training modules for OIG staff in areas of particular interest to the OIG.

Appendixes

Appendix 1
Audit Reports Issued with Questioned Costs for the Period April 1 through September 30, 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 April 1 through September 30, 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	09/08	3	0
Audit of Retirement Plan Administration	07/03	4	3	1	03/08	3	1
Audit of the Board's Fixed Asset Management Process	05/05	2	2	0	09/08	2	0
Evaluation of Service Credit Computations	08/05	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	09/08	1	1
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	–	–	–
Audit of the Board's Information Security Program	09/08	2	2	0	–	–	–
Control Review of the Board's Currency Expenditures and Assessments	09/08	6	6	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 Reporting Requirements of the Inspector General Act, as amended, for the Reporting Period:

Section	Source	Page(s)
4(a)(2)	Review of legislation and regulations	22-26
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	20
5(a)(5)/6(b)(2)	Summary of instances where information was refused	None
5(a)(6)	List of audit reports	5-10
5(a)(7)	Summary of significant reports	None
5(a)(8)	Statistical Table—Questioned Costs	33
5(a)(9)	Statistical Table—Recommendations that Funds Be Put to Better Use	34
5(a)(10)	Summary of audit reports issued before the commencement of the reporting period for which no management decision has been made	35
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, U.S. Department of the Treasury
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
CBO	Carrier Billing Online
CCIG	Council of Counsels to the Inspector General
CIO	Chief Information Officer
COS	Currency Ordering System
ECIE	Executive Council on Integrity and Efficiency
EOF	External Oversight Function
ESS	Electronic Security System
FDIA	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FRB BOSTON	Federal Reserve Bank of Boston
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GPO	Government Printing Office
GSS	General Support System
GTC	Government Travel Card
IG Act	Inspector General Act of 1978
IT	Division of Information Technology
LEU	Law Enforcement Unit
MGT	Management Division
MLR	Material Loss Review
NED	National Examination Database
NIST	National Institute of Standards and Technology
OEB	Office of Employee Benefits
OIG	Office of Inspector General
PCIE	President's Council on Integrity and Efficiency
PII	Personally Identifiable Information
RBOPS	Division of Reserve Bank Operations and Payments Systems
SI	Smithsonian Institution
S&R	Supervision and Regulation
SRC	Supervision, Regulation, and Credit

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

or visit our electronic hotline at:
http://www.federal reserve.gov/oig/oig_hotline_hl.htm


BOARD OF GOVERNORS
THE FEDERAL RESERVE SYSTEM