A Progress Report To The President

President's Council on Integrity and Efficiency

Executive Council on Integrity and Efficiency

Fiscal Year 1999

UNITED STATES of AMERICA
PCIE
PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY

UNITED STATES of AMERICA
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY

CONTENTS

FOREWORD

The Inspector General (IG) community was a very positive and powerful force in the federal government during Fiscal Year (FY) 1999. This report attests to the excellent progress made by the member Offices of Inspector General (OIG) of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) in carrying out the mission of the inspector general established by the Congress in October 1978.

Facing the unprecedented technological challenge of Year 2000, the IG community responded by partnering with agency management and, in large part due to intensive joint efforts of these groups, the federal government successfully ushered in the millennium. Understanding and keeping pace with real and potential threats to the systems and data supporting essential federal operations, the IG community tackled a number of cross-cutting systems security issues and offered valuable technical advice. OIGs throughout the federal government also advanced congressional emphasis on improving agencies' strategic planning and maximizing results by sharing best practices and recommending better ways of implementing the Government Performance and Results Act during FY 1999. Through hundreds of independent and objective audits, investigations, and evaluations of federal programs and activities, OIGs effectively promoted financial management accountability, helped ensure integrity, minimized risks of fraud and abuse, and produced results: potential savings of more than $8.2 billion, actions to recover over $4 billion, over 13,000 successful prosecutions[1], suspensions or debarments of nearly 6,700 individuals or businesses, and over 1,224 civil actions.

This progress report is rich with individual examples of these accomplishments, and every OIG represented should be proud of the achievements presented in the Executive Summary and discussed in detail later in this report. However, in our view, it is the progress of the IG community taken as a whole that matters most. We worked at continuing to reinvent ourselves. We combined forces to confront common challenges more effectively and efficiently. We improved communications with one another and with our agency management as we pursued solutions to complex technological and other pressing issues. We used innovative audit and investigative approaches in conducting our work, striving continually to improve the quality and usefulness of our products. We formed even stronger alliances within the IG community and more importantly with the U.S. General Accounting Office (GAO), the Office of Management and Budget (OMB), and the Congress. Such cooperation is a fundamental component of OIG endeavors and is critical to our success.

We express our gratitude to every individual working to foster the goals of the IG community. Generally, our members come from 57 OIGs and provide oversight for 59 federal agencies. Our community is a professional, dedicated, and diverse group with training, experiences, and talents that we feel privileged to contribute to the federal government. We also extend our appreciation to agency management across the government and to the Congress for their continued support of our many and varied activities in the audit, investigative, and evaluative arenas.

[1] Includes investigative results from the Postal Inspection Service overseen by the U.S. Postal Service Office of Inspector General.

The results of much of our work during FY 1999 will have long-lasting impact. We also hope to build on our past success as we plan our future work. To that end we are developing the first ever comprehensive PCIE/ECIE Strategic Plan which will guide our efforts in the years ahead. The focus of our Strategic Plan will be to contribute to the long-term efficiency, integrity, and effectiveness of the federal government. Moreover, our plan will be flexible enough to address the concerns of coming Administrations, the Congress, and emerging risks facing the federal government in the future.

As a community, we enter the Year 2000 united and prepared to meet new challenges. We are committed to carry out the vision of the Congress in establishing Offices of Inspector General, add maximum value to federal programs and activities, and sustain the close working relationships that have served us well during the past year.

Gaston L. Gianni

Gaston L. Gianni, Jr., Vice Chair
President's Council on
Integrity and Efficiency

Barry R. Snyder

Barry R. Snyder, Vice Chair
Executive Council on
Integrity and Efficiency

EXECUTIVE SUMMARY

The following discussion summarizes the overall results included in this Progress Report. We have organized our results under three categories that reflect important themes of OIG work during FY 1999: Information Technology; the Government Performance and Results Act; and Integrity, Accountability, and Results.

IG Community Addresses Critical Information Technology Issues

During FY 1999, the OIGs focused unparalleled attention on information technology issues, from providing real-time assistance in ensuring the government's readiness for the century date change to helping agencies achieve systems integrity and continuity of operations in their technology infrastructure and information networks. As evidenced by the wide-ranging accomplishments highlighted in this report, the IG community has not only successfully used the more traditional audit and investigative approaches to achieve results, but has also placed increased emphasis on proactive partnerships with management, shared best practices, and employed new investigative and analytical tools.

The results have been impressive. The OIGs played a pivotal role in the smooth transition to the Year 2000 (Y2K), helping agencies either correct potential problems or effectively implement contingency plans. Agencies also made progress in identifying security vulnerabilities; developing and implementing controls to strengthen information systems security; and providing essential back-up, recovery, and contingency plans to restore operations in the event of a system failure — in large part due to the OIGs' sustained commitment to ensuring systems integrity.

OIGs Help Ensure the Government's Readiness for Year 2000

Mitigating the risks associated with the Y2K computing problem was one of the most time-critical challenges facing the nation during FY 1999, and the OIGs invested substantial resources in helping federal managers successfully meet the challenge. The OIG at one major department, for example, conducted 180 audits on Y2K conversion efforts, the most extensive auditing of a non-financial subject in the department's history. Recognizing the significant risks of system failures and business interruptions, many OIGs engaged in a "real-time" dialogue with agency management on pressing issues such as the readiness of mission-critical systems and the quality of contingency planning. These investments led to many positive results, which include:

- Providing senior managers and commanders in the U.S. military with reliable and timely feedback about the military's Y2K readiness efforts and potential security ramifications;

- Preparing mission-critical systems supporting air traffic control, searches and rescues involving ships, and safety inspections for a smooth transition to the new millennium;

- Building collaborative partnerships to mitigate successfully Y2K disruption in the banking and financial services industry; and

- Ensuring that the computer systems used by Medicare contractors to process and pay approximately $180 billion in fee-for-service claims each year would operate effectively in the Year 2000 and beyond.

To also ensure successful preparation for the Year 2000, the IG community established and maintained strong alliances with GAO, OMB, and the Congress, all of whom were actively monitoring agencies' progress in becoming Y2K compliant. A number of Inspectors General testified on Y2K issues before congressional committees.

More specific examples of the IG community's effectiveness in meeting the Year 2000 challenges are presented in Section I.A. of this report.

OIGs Promote Systems Security

The global expansion of information technology has introduced new risks and threats to the systems and data supporting many essential federal operations, and the IG community has continued to emphasize the need to protect the government's technology infrastructure and information networks from unauthorized access and disruption. Although maintaining systems security and integrity has been a longstanding and complex issue, the IG community is committed to keeping pace with emerging technological risks and is making great strides in identifying vulnerabilities and strengthening systems integrity both collectively and in respective agencies. For example, the OIGs are working collaboratively to focus attention on critical infrastructure issues raised in Presidential Decision Directive 63 (May 1998) which called for a nationwide effort to ensure the security of those physical and cyber-based systems essential to the minimum operations of the economy and government. At their respective agencies, the OIGs have been instrumental in helping their agencies take a more proactive role in managing risk and strengthening systems security. Section I.B. of this progress report contains numerous examples of the IG community's impact on this issue, including the following:

- Providing a comprehensive and cumulative assessment of systems security vulnerabilities associated with the military's 10,000 networks and 1.5 million computers that emphasizes more innovative and lasting solutions to long-standing issues;

- Recommending controls and other measures to eliminate or mitigate several information technology security breaches;

- Improving controls over sensitive taxpayer data files; and

- Strengthening controls to protect agency systems from the disruption and damage caused by computer viruses.

IG Community Plays Key Role in Results Act Implementation

Over the past year, the Inspector General community has been a key player in the steady implementation of the Government Performance and Results Act (GPRA). Enacted in 1993, GPRA called for a significant change in the way the government does its business. GPRA requires most federal agencies to develop a strategic plan that defines its mission and vision, an annual performance plan that translates the strategic plan into measurable objectives, and an annual performance report that compares actual results against planned goals. Simply put, federal programs will set targets for their accomplishments and then be evaluated on the basis of actual results. The first annual performance reports are due to the President and the Congress in March 2000.

Through a variety of approaches, the community has made a difference. Many IGs have developed partnerships with their agencies to oversee GPRA implementation and act as advisors, and at times working-group participants, to further facilitate the process. The work of the community-based GPRA Coordinators Interest Group has allowed OIGs to leverage their knowledge and experience and share "best practices" with their agencies. This group, originated and chaired by the Department of State OIG, has been supporting its more than 100 members for the past two years with GPRA information, speakers, and training.

During FY 1999, the community has conducted numerous audits and other reviews to identify areas where their respective agencies could improve upon GPRA implementation. The majority of the attention this year was directed, in general, at performance measures, and more specifically, at systems and data integrity and reliability. The fruits of the government's labor can be effectively measured only if the data and the systems providing the data can be relied upon. During the year, several OIGs issued reports identifying opportunities to improve internal controls that would ultimately improve performance measurement data. Numerous other OIGs issued reports recommending ways to enhance data reliability unique to the individual agency program.

Section II of this report discusses the IG community's GPRA efforts in more detail.

IG Community Helps Ensure Integrity, Accountability, and Results

During the past year, the work of the IG community government-wide has contributed to the integrity of federal programs and activities, increased the accountability of financial and managerial operations, and produced results that have positively impacted the beneficiaries of federal programs. The audits, inspections and evaluations, investigations, and legislative activities of the IG community have resulted in potential savings of more than $4.0 billion and actions to recover more than $3.0 billion in federal monies. Additionally, the OIGs conducted investigations that resulted in more than 13,000[2] successful prosecutions, suspensions or debarments of more than 6,600 people or businesses, and more than 1,200 civil actions. Through the OIGs' efforts, all of the major agencies have received financial audits of their respective financial statements and many have merited unqualified or "clean" audit opinions. The OIGs have also been instrumental in the integration of the agency financial statements into a consolidated annual financial statement that provides a broad picture of the fiscal activities and further accountability of the finances for the entire federal government.

Just as important as the financial oversight of federal operations, the OIGs have identified illegal activities or mismanagement in federal programs. The OIGs' report recommendations have been the catalyst to changes in federal agencies' policies and

[2] Includes investigative results from the Postal Inspection Service overseen by the U.S. Postal Service Office of Inspector General.

practices for providing better and more efficient services, improving safety and security, or focusing on the needs of the American public in the areas of crime, health care, education, housing, the environment, banking, and other areas. For example, OIG work has resulted in:

- Upgrading security equipment and other security measures in federal buildings;
- Enhancing road safety by heightened attention to trucking violations;
- Deterring potential crimes by curbing inmates' use of prison telephones;
- Increasing oversight of health care providers submitting bogus claims;
- Obtaining water and sewer connections for poor households in a Texas community;
- Accelerating the incineration of toxic wastes; and even
- Strengthening the monitoring of large and complex banking institutions that are taking increased risks with the public's money.

Additional examples of the IG community's impact on the integrity, accountability, and results of federal programs, functions, and activities are presented in Section III of this report.

Additional Information

In addition to our work in the three areas outlined above, our progress report contains an introduction on the IG role and community, a discussion of PCIE/ECIE committees and projects, and statistical tables showing monetary results as well as other actions related to investigative activities. Our report also provides the reader a PCIE/ECIE membership directory and a glossary of terms, which we hope are helpful.

PROFILE OF PERFORMANCE — FISCAL YEAR 1999

Summary of Combined Statistical Accomplishments By PCIE and ECIE Members

Recommendations that Funds Be Put to Better Use	**$12,548,658,272**
Management Decisions on Recommendations That Funds Be Put to Better Use	**$ 8,232,422,622**[3]
Questioned Costs	**$ 4,107,653,322**
Management Decisions on Questioned Costs	**$ 2,257,869,605**
Successful Criminal Prosecutions	**13,064**[4]
Civil Actions	**1,224**
Personnel Actions	**1,224**
Suspensions/Debarments	**6,682**
Investigative Recoveries	**$ 1,765,059,109**

[3] Includes recommendations from prior years.

[4] Includes investigative results from the Postal Inspection Service overseen by the U.S. Postal Service Office of Inspector General.

THE INSPECTOR GENERAL COMMUNITY

In October 1978, Congress passed the Inspector General Act of 1978, which created independent audit and investigative offices within 12 federal agencies. Before that time, most federal audit and investigative resources were under the management of specific federal program offices–meaning that federal auditors and investigators were frequently under the direction of the programs they were reviewing. This splintered system also made it hard for these small audit and investigative offices to see a pattern of abuse against their agency's programs.

The Inspector General (IG) concept has proved to be of significant benefit to the government. Each year billions of dollars are returned to the federal government or better spent based on the recommendations from IG reports. Because of this success, the IG concept has been gradually expanded to most of the federal government. In FY 1999, there were 57 OIGs providing oversight to 59 federal agencies and entities (hereinafter "agencies" for ease of reference).

"Inspector General" may seem an unusual name for a civilian auditor/investigator. The modern civilian IG was derived from the military custom of having an independent "Inspector General" to provide an independent review of the combat readiness of the Continental Army's troops. Today's civilian IGs are charged with a similar mission: to independently review the programs and operations of their agencies; to detect and prevent fraud, waste, and abuse; and to promote economy, efficiency, and effectiveness so that their agencies can best serve the public.

Independence. The major way IGs are different from other federal officials is their independence. This statutory independence is meant to ensure the impartiality of IG audits and investigations.

The Inspector General Act authorizes IGs to:

- Conduct such investigations and issue such reports as they believe appropriate (with limited national security and law enforcement exceptions);
- Issue subpoenas for information and documents outside the agency (with the same limited exceptions);
- Have direct access to all records and information of the agency;
- Have ready access to agency heads;
- Administer oaths for taking testimony;
- Hire and control their own staff and contract resources; and
- Request assistance from any federal, state, or local government.

IGs report both to the head of their respective agencies and to the Congress. This dual reporting responsibility is the framework within which IGs perform their functions. Unique in government, it is the legislative safety net that protects the IGs' independence and objectivity.

IGs are interested in input on what projects they should pursue. Except in special circumstances, IGs share drafts of their reports with their agencies and respond to agency comments in final reports. IGs also frequently provide "technical advice" on a particular issue or piece of legislation to officials within their agencies and to Members of Congress. Many IGs participate in their agencies' senior councils, and frequently OIG staff provide advice to agency "reinvention councils" as management policies are developed.

Mission. In simple terms, the IGs have two basic roles: to find and report on current problems, and to foster good program management to prevent future problems. This report describes many examples of how the OIGs meet their specific statutory mission to:

- Conduct and supervise audits, investigations, and inspections relating to the programs and operations of their agencies;
- Review existing and proposed legislation and regulations relating to the programs and operations of their agencies;
- Provide leadership for activities designed to promote economy, effectiveness, and efficiency and fight fraud, waste, and abuse in their agencies' programs; and
- Inform their agency heads and the Congress of problems in their agencies' programs and operations and the necessity for and progress of corrective actions.

In performing this mission, the IGs prepare a variety of reports, including the following.

Audit Reports. Most OIG resources are spent on audits. OIG audits evaluate:

- Performance of agency programs and supporting administrative and financial systems;
- Compliance with relevant laws and regulations;
- Whether there are ways that funds could be put to better use;
- Whether contractors and/or grantees have met their responsibilities to the government; and
- Whether people or firms doing business or receiving benefits from the government have received funds to which they are not entitled and should make restitution.

By law, OIG audits are performed under auditing standards set by GAO.

OIGs devote the bulk of their resources to audits and related services. This work is performed by OIG audit staff, other federal auditors under cost-reimbursable agreements, or nonfederal auditors under various contracting or partnering arrangements.

Inspection Reports. Inspections are similar to policy and program evaluations. Several of the OIGs have adopted inspections as a quick way to spot test the effectiveness of their agency programs or to do a broad review on issues affecting agency programs. The PCIE and ECIE have adopted professional standards to ensure the validity and independence of IG inspections.

In FY 1999 alone, OIG audits and inspections led to managers making decisions to better spend more than $8.2 billion and to seek the return to the government of more than $2.2 billion.

Investigation Reports. In accordance with professional standards and guidelines established by the Department of Justice (DOJ), OIGs perform investigations of both criminal and administrative wrongdoing against agency programs. When they deem necessary, IGs investigate outside beneficiaries, contractors or grantees, or federal officials — indeed, IGs are empowered to investigate anyone who may have defrauded their agencies' programs. IGs are required to report suspected violations of criminal law directly to the Attorney General and frequently work cooperatively with DOJ on criminal investigations. In FY 1999 alone, OIG investigations led to the recovery of almost $1.8 billion, more than 13,000[5] successful prosecutions, the suspension or debarment of more than 6,600 people or businesses doing business with the government, and more than 1,200 civil actions.

Semiannual Reports to Congress. These reports are specifically required by the Inspector General Act. IGs must summarize their most significant recent reports and management's action on significant IG recommendations. These reports provide a useful overview of OIG activity and demonstrate the value each IG contributes.

IG Appointments. IGs are appointed on the basis of their personal integrity and their expertise in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations. The IGs serving at the cabinet-level departments and major sub-cabinet agencies are nominated by the President and confirmed by the Senate. These IGs can be removed only by the President. IGs at smaller independent agencies, corporations and other federal entities — called "designated federal entities" — are appointed the heads of those entities, who can also remove them from office. In either case, both houses of Congress must be notified of the reasons for removal.

PCIE. The Presidentially appointed IGs work together and coordinate their professional activities through the President's Council on Integrity and Efficiency (PCIE), which was created by an Executive Order dated March 26, 1981, and updated in 1986 and 1992. The PCIE works to promote collaboration on integrity, economy, and efficiency issues that transcend individual governmental agencies and to increase the professionalism and effectiveness of IG personnel throughout the government. The Deputy Director for Management of OMB, who is responsible for reporting to the President on its activities, chairs the PCIE. In addition to the Presidentially appointed IGs, members include the Controller of the Office of Federal Financial Management at OMB, the Special Counsel of the Office of Special Counsel (OSC), the Director of the Office of Government Ethics, the Deputy Director of the Office of Personnel Management (OPM), and a representative of the Director of the Federal Bureau of Investigation (FBI).

Most of the work of the PCIE is done by its committees. That work is summarized later in this report. The PCIE also maintains two training centers for OIG staff: the Inspectors General Auditor Training Institute at Fort Belvoir, Virginia, and the Inspector General Criminal Investigator Academy at the Federal Law Enforcement

[5] Includes investigative results from the Postal Inspection Service overseen by the U.S. Postal Service Office of Inspector General.

Training Center at Glynco, Georgia. PCIE members also join together in a number of substantive working groups, including the Government Performance and Results Act Roundtable and the Information Technology Roundtable.

ECIE. The Executive Council on Integrity and Efficiency (ECIE), comprised primarily of the IGs appointed by designated federal entity heads, was created by Executive Order on May 11, 1992. The ECIE has the same mission as the PCIE: address integrity and efficiency issues that transcend individual government agencies and increase the professionalism and effectiveness of IG personnel throughout the government. The Deputy Director for Management of OMB chairs the ECIE. In addition to the IGs, members include the Special Counsel of OSC, Director of the Office of Government Ethics, the Deputy Director of OPM, and the Assistant Director, Criminal Investigative Division of the FBI. The ECIE also has representatives on PCIE committees.

You can find information on PCIE, ECIE, and individual OIG work on the IG community web page, known as IGNet, located at http://www.ignet.gov.

This report summarizes some of the more significant results of OIG audits, inspections, and investigations during FY 1999. The examples provided are grouped into the following subject areas:

- Information technology, including Year 2000 and systems security;
- Government Performance and Results Act; and
- Integrity, accountability, and results.

I. INFORMATION TECHNOLOGY

A. Helping Ensure Government's Readiness for Year 2000

FY 1999 was a time of intense preparation for a year of unprecedented numerical significance. The potential for systems-induced disruptions on a global scale led managers across the nation, and indeed around the world, to launch concerted efforts, unparalleled in scope and intensity, to ensure that information systems would continue to deliver accurate, timely information as the 21st century began. Throughout the federal government, OIGs worked with managers and officials in their agencies to ensure that federal information systems would successfully meet the challenge. Following are examples of Inspectors General efforts during FY 1999 to ensure that government systems were ready to deliver efficient and effective products and services on January 1, 2000.

Commerce OIG Focuses on Reducing Risk of Y2K Failures and Business Interruptions

The OIG served an important function by ensuring that Department of Commerce (DOC) business operations and computer systems were ready for the Year 2000 by reviewing both departmental leadership and individual bureaus' Y2K programs. In FY 1999, the OIG reviewed six DOC bureaus. Through these reviews, discussions with the chief information officer (CIO) and interactions with the Department's Y2K working group, the OIG raised senior managers' concern about the efficacy of their Y2K programs.

Responding to OIG recommendations, DOC officials directed bureaus to develop comprehensive critical systems inventories, prioritize systems renovation activities, and substantiate systems compliance through test documentation and independent systems validation. DOC also increased monitoring of bureau progress by requiring bureau managers to brief the CIO. The bureaus agreed to complete systems inventories and establish policies for managing change to Y2K-compliant systems. They also agreed to update business continuity and contingency plans with additional analysis of Y2K failure scenarios, to test contingency plans, and to start contingency activities that must be completed before the century change. *(DOC)*

OIG Conducts Historic Audit of DoD Year 2000 Conversion Efforts

The Department of Defense (DoD) OIG conducted 180 audits on DoD Year 2000 conversion efforts, the most extensive auditing of a non-financial subject in the department's history. Most reports with audit findings about the accuracy of management progress reports and about testing, contingency planning, supplier outreach, security ramifications, and host nation Year 2000 status abroad were issued during FY 1999, including three reports on U.S. Forces Korea.

The series of Korea audits provided senior managers and commanders with reliable and timely feedback about Year 2000 readiness efforts of the several commands in that theater of operations. This input was critical, as the U.S. military must maintain a very high readiness level because of the political situation on the peninsula. Those efforts initially lagged, and the audits became a catalyst for initiating more effective action within U.S. commands and between U.S. and Republic of Korea officials. The Korean Government issued a press release noting the important role that auditors played in facilitating better coordination between the Y2K coordinators and the respective government's base commanders. In addition, the auditors provided constructive advice about how to improve Year 2000 systems integration testing and contingency planning. *(DoD)*

OIG Advisory Documents Help Focus DOE Remediation Efforts

The Department of Energy (DOE) OIG continued an ongoing collaboration with the agency's CIO in FY 1999 to resolve DOE's Year 2000 computer problems. This effort culminated in the issuance of three advisory memoranda to the Deputy Secretary, providing significant contributions in the areas of project management, mission critical system inventory, contingency planning, data exchanges, embedded systems, and test plans. These reports emphasized important fundamental issues that provided a focus for DOE remediation efforts. Indeed, the CIO used the OIG's work to facilitate and expedite DOE's remediation efforts. *(DOE)*

OIG Audits Lead DOI to Take Action on Potential Y2K Problems

At the request of the agency's CIO, the Department of the Interior (DOI) OIG conducted audits to determine whether DOI bureaus: 1) inventoried select automated information systems and identified mission-critical systems that were not Y2K compliant; 2) developed auditable cost estimates for renovating systems to be Y2K compliant; 3) identified, by name, individuals responsible for ensuring that bureaus are Y2K compliant; 4) ensured that responsible individuals' personnel performance evaluation plans included critical elements related to identifying and remedying Y2K problems; 5) developed a credible plan that included milestones and a critical path to ensure that the bureaus are Y2K compliant; and 6) developed a contingency plan that would address the failure of any part of DOI systems to be Y2K complaint. Subsequent to the audits, each audited bureau reported that they had completed action on all six of the identified areas. *(DOI)*

DOJ OIG Identifies Weaknesses in Several Key Areas

The Department of Justice OIG issued Y2K reports in three key areas. An OIG audit of Justice Data Centers (JDC) in Rockville, Maryland and Dallas, Texas found that: 1) not all JDC-maintained software tools and utilities were Y2K compliant; 2) Y2K contingency plans were not developed; and 3) Y2K testing of hardware, operating systems, and software tools and utilities were not performed. During an audit of the Y2K oversight process, the OIG found that although department components had primary responsibility for their own Y2K fixes, the DOJ Justice Management Division monitored and reported the status of mission-critical computer systems. This audit disclosed that the Department had not consistently established how many systems it had to fix, their status, and related costs. A third audit focused on the effectiveness of the Drug Enforcement Administration's initiatives on the Y2K computer problem. After each audit, the department took steps to address identified weaknesses. *(DOJ)*

OIG Reviews Help DOT Identify Y2K Issues

Since the OIG performed the first of nine Y2K reviews in 1997, the Department of Transportation (DOT) has done a great deal to prepare for the Year 2000, but at the end of FY 1999, tasks remained for a smooth transition to the new millennium. Of 609 mission-critical systems — used to support such functions as air traffic control, searches and rescues involving ships, and safety inspections — 310 required Y2K repairs, and all 310 systems have been fixed. Included were 152 aviation-related systems, 87 maritime systems, 34 related to surface transportation, and 37 other supporting systems.

The OIG attributed the success of this undertaking to strong congressional oversight, leadership by the Secretary and Deputy Secretary of Transportation and modal administrators, and hard work by DOT employees. In September 1999, testifying before the Senate Special Committee on the Year 2000 Technology Problem, the OIG identified areas in which further preparedness was needed to guarantee a smooth transition into the 21st century. *(DOT)*

OIG's Y2K Recommendations Continue to Show Significant Results at EPA

The Environmental Protection Agency (EPA) OIG was among the first agency entities to identify the Y2K vulnerability and assess the potential impact on programs and operations. During FY 1999, OIG performed oversight by monitoring the conversion process and commenting on the independent certification program and independent verification and validation draft (IV&V) reports for EPA's mission-critical systems. OIG also reviewed the OMB Quarterly Y2K Status Reports and briefed GAO representatives and congressional subcommittees about the reliability of data included in these reports.

As a result of OIG recommendations, advisory services, and dedicated management, EPA made significant progress toward positioning its information technology assets to transition successfully to the upcoming calendar year. For example, the CIO implemented a comprehensive certification program requiring senior officials to formally certify Y2K compliance of all assets under their control, subject to independent testing and certification administered through an interagency agreement with DOT. Additionally, EPA developed a business continuity and contingency plan methodology that drives the planning, testing, and implementation of contingency procedures for the agency's core business processes. *(EPA)*

OIG Efforts to Ensure FDIC's Y2K Readiness are Comprehensive and Continuous

During FY 1999, the Federal Deposit Insurance Corporation (FDIC) OIG engaged in a comprehensive assessment of the FDIC's efforts to ensure Y2K readiness of both the financial institutions it supervises and its internal systems. The OIG's approach to this work was to communicate continuously with management through briefings and advisory memoranda on a real-time, proactive basis.

The OIG reviewed all phases of the supervisory and internal Y2K efforts to ensure that management adhered to a rigorous and structured approach to decrease its Y2K risks. As part of its review of the supervisory Y2K efforts, the OIG visited 27 field offices to ensure that Y2K examination results, ratings, and oversight of financial institutions were accurate, complete, and consistent. The OIG reviewed the corporation's customer awareness efforts and contingency and Y2K event management plans, as well as the timeliness, accuracy, and integrity of data contained in its tracking system. The OIG also summarized and presented to FDIC management "best practice" suggestions observed during its nationwide review. With respect to the corporation's internal efforts, the OIG focused on Y2K program costs, readiness of mission-critical systems, Y2K certification of systems, configuration management, the FDIC's business continuity and contingency plan, and contingency planning. At year-end, the OIG was present at the corporation's communication centers to observe rollover events and activities. *(FDIC)*

OIG Notes Significant Progress by AID to Mitigate Y2K Risks, But Problems Remain

OIG audits during FY 1999 revealed that, after a slow start, the Agency for International Development (AID) made significant progress to mitigate Y2K risks. Ongoing work, however, showed continuing deficiencies. In testimony before the House International Relations Committee about the adequacy of AID's Y2K contingency plans, OIG stated that AID had developed a contingency plan for key financial management functions, including obligating and controlling funds, and making payments. AID, however, had not developed contingency plans for some core business functions needed to continue providing development assistance.

The OIG also continued to monitor AID's efforts to ensure that its computer systems could correctly process Year 2000 dates. While AID reported to OMB that all seven agency mission-critical computer systems were Y2K ready, OIG's review of two systems disclosed that some tests were not completed, while others were not well documented. AID has been very responsive to OIG's findings and has generally taken action to correct deficiencies as they are identified. *(AID)*

OIG Spurs USDA Toward Year 2000 Compliance

To ensure Y2K readiness, embedded chips in vulnerable systems and processes (VS&P) must be addressed. At the end of the first half of FY 1999, the Department of Agriculture (USDA) OIG found that overall, USDA had not yet determined the full extent of its VS&P and telecommunications-equipment Y2K problem because inventories had not been completed and assessment procedures had not been fully disseminated. Also, no audited sites had a formal process for certifying that equipment was Y2K compliant. Responsible personnel concurred that additional guidance was needed to ensure adequate and accurate progress toward completing USDA's efforts. In addition, approaching the end of the FY, the OIG found that not all USDA agencies were adequately documenting system validation efforts or having IV&V reviews performed for each of the departmental priority systems.

Prompted by the OIG's concerns, USDA's CIO immediately reinstructed the agencies regarding the importance of appropriately documenting all phases of testing activities, and required the agencies to, at a minimum, conduct an IV&V for each of the departmental priority systems. *(USDA)*

FEMA Makes Progress in Compliance Efforts but Needs to Lessen its Vulnerability

The Federal Emergency Management Agency (FEMA) OIG reviewed the agency's process for evaluating hardware, software, and building infrastructure equipment to determine whether computers and other equipment would continue to function properly in the Year 2000. The OIG determined that FEMA was making progress by developing a framework for meeting compliance requirements. FEMA also established: 1) a process for reviewing building infrastructure equipment; 2) a project management structure that assigned responsibilities for each information system, software application, data exchange, and network server; 3) an independent validation process for verifying system administrators' test results; and 4) a centralized process for coordinating and preparing reports for internal and external distribution.

Although FEMA was progressing in its compliance efforts, OIG identified other actions needed to lessen its vulnerability. Specifically, FEMA needed to ensure that: 1) mission-critical systems were corrected and tested before March 31, 1999; 2) commercial off-the-shelf software and computers were evaluated properly; 3) FEMA building infrastructure equipment was compliant; and 4) adequate plans were developed to address system contingencies and business continuity. FEMA agreed and began corrective actions. *(FEMA)*

OIG Finds Weaknesses in Renovation, Testing, and Certification at HUD

The Department of Housing and Development (HUD) OIG issued two audit reports during the year on HUD's Y2K initiative. The first report emphasized that senior-level officials needed to be involved in managing and coordinating Y2K activities, and noted that the CIO does not have direct authority over the Office of Information Technology and contractor personnel performing Y2K work. As a result, the OIG found weaknesses in the renovation, testing, and certification processes. The audit disclosed that: 1) project and test plans did not provide sufficient details for management to monitor and control the Y2K conversion process; 2) software renovation lacked a controlled process to ensure that all date fields were identified for changes; 3) testing standards were not sufficient to ensure adequate test coverage; and 4) the certification process did not include an independent assessment of testing adequacy. The second report found deficiencies in Y2K contingency plans, Y2K preparedness at the data center and building facilities, and end-user Y2K computing compliance. *(HUD)*

OIG's Visits to HHS/HCFA Contractors Focus on Systems Readiness

In assessing the Department of Health and Human Services' (HHS) progress toward Y2K computer system readiness, OIG's focus has been on the Medicare program, in particular the readiness of Medicare contractor systems and the external systems that interact with those of the Health Care Financing Administration (HCFA). This HHS agency administers the Medicare program through a network of contractors, generally insurance companies, that process hospital and other provider claims for payment.

Because the Medicare contractors process and pay about $180 billion in fee-for-service claims each year, the ability of their computer systems to operate effectively by Y2K and beyond is of critical importance. By the end of FY 1999, OIG staff participated in 360 visits to the contractors, along with staff from HCFA and its independent verification and validation contractor. These visits focused on contractors that maintain systems shared by claims processing contractors and on data-processing centers used by multiple contractors to process Medicare claims. The OIG not only evaluated the progress of remediation efforts, but also addressed such concerns as inadequate contingency plans to deal with possible system failures and the need for additional guidance from HCFA on testing requirements. *(HHS)*

OIG Recommendations Help NASA Assure Its Ability to Respond to Y2K-related Failure

During FY 1999, the National Aeronautics and Space Administration (NASA) OIG completed seven audits on NASA's efforts to resolve Y2K issues. These audits addressed the agency's efforts using the five-phase model developed by OMB: awareness, assessment, renovation, validation, and implementation. While NASA's overall Y2K efforts were satisfactory, the OIG reported the following concerns: 1) inadequate support for Y2K cost estimates reported to OMB; 2) inadequate documentation of Y2K work performed on selected mission-critical systems; 3) inadequate sharing of information on the status of commercial-off-the-shelf products; 4) lack of reasonable assurance that contractors would provide Y2K-compliant data to support NASA's key financial and program management activities; 5) lack of reasonable assurance that research results from grants and cooperative agreements would not be adversely affected by Y2K problems; 6) failure to incorporate NASA-directed Y2K requirements into applicable IT operations and maintenance contracts, and to request an exemption for completing system testing that deviated from Y2K testing and certification guidelines and requirements; and 7) inadequate NASA test plan guidance and contingency planning and testing. Except for the issue involving Y2K cost estimates, which was ultimately resolved, management concurred and agreed to take corrective actions on all recommendations. *(NASA)*

OIG Provides Extensive Feedback to NRC on Nationwide Y2K Contingency Plan Exercise

The Nuclear Regulatory Commission (NRC) OIG evaluated NRC’s progress toward resolving the Y2K issue to help ensure the agency would continue to meet its established goals. The audit staff worked closely with agency officials and outside entities to ensure that licensees’ efforts were adequate to protect public health and safety, and that NRC’s internal systems were compliant. Throughout its monitoring of NRC’s internal and external efforts, OIG continually provided real-time feedback and suggestions to management and staff on issues. OIG watched the agency undergo a nationwide Y2K contingency-plan exercise for responding to occurrences at reactor licensees during the transition. OIG provided extensive feedback to NRC about the exercise, including raising questions about the roles of key NRC officials during the rollover. The agency used the feedback, along with other input, to strengthen contingency plans overall. *(NRC)*

OIG Recommends Corrective Actions for Numerous Y2K Problems at IRS

The Y2K problem was complicated by the size, complexity, and interdependencies of the Internal Revenue Service’s (IRS) computer systems, particularly for an organization as large and as reliant on computers as the IRS. The Treasury Inspector General for Tax Administration’s (TIGTA) review of IRS' contingency plans indicated that IRS had not devoted sufficient emphasis to contingency planning. The database used for tracking the conversion process was inaccurate; unreliable data hindered IRS management's ability to monitor conversion progress, and prepare contingency plans for systems at risk of not meeting conversion deadlines. Even when data did identify systems at risk, IRS management did not follow its own processes, and did not ensure that contingency plans were developed in a timely manner. In addition, IRS had not properly coordinated contingency-planning efforts with overall contingency-planning efforts for disasters and other types of failures.

The OIG recommended several corrective actions, including: reviewing Y2K inventory files on a recurring basis; establishing validity checks; establishing procedures to identify and monitor components and systems that had not completed Y2K milestones; and establishing procedures to identify "at risk" systems during the certification process. *(TIGTA)*

OIG Finds RRB's Y2K Plans on Track

The Railroad Retirement Board (RRB) OIG conducted ongoing reviews of RRB's Y2K project involving the conversion of 160 mainframe and 70 personal computer (PC) application systems. The OIG determined that RRB's Y2K project management was adequately administered, controlled, and allowed for timely completion. Auditors reviewed the inventory of critical (essential to the RRB's mission of paying benefits to the railroad community) and non-critical systems and found the rating of systems reasonable. Review results indicated that RRB established an appropriate plan to ensure that its systems were compliant. RRB completed conversion of all mission-critical systems in January 1999, and accelerated completion of all non-mission-critical systems. At the end of the FY, the RRB had completed conversions of 95 percent of all mainframe systems and 100 percent of PC systems. *(RRB)*

OIG Engages in Comprehensive Effort to Promote DOS's Y2K Readiness Worldwide

The Department of State (DOS) OIG's certification reviews provided DOS management during FY 1999 with the documented assurance they needed for the Y2K compliance of mission-critical systems. OIG was also actively engaged in the international Y2K arena through readiness assessments conducted during visits to 26 countries. OIG testified twice on global Y2K readiness issues before the Senate Special Committee on the Year 2000 Technology Problem, and drew attention to the need for a cohesive framework for U.S. Y2K policy issues and a global approach to addressing Y2K contingency planning.

OIG assisted in establishing a process through which the department certified the Y2K compliance of its mission-critical systems, by writing detailed guidelines that each bureau used in developing application-certification packages for submission to the Y2K Program Management Office, and OIG. The certification process provided the department's senior management with assurance that every feasible effort had been made to prevent Y2K-related failures on January 1, 2000. OIG also issued a management letter to the Chairman of the Broadcasting Board of Governors (BBG) concerning the Y2K readiness of the affiliates used by the international broadcasters under BBG's purview. OIG recommended that the BBG direct all of the entities under its control to randomly survey their affiliates to determine their Y2K readiness. The BBG agreed with the recommendations and took steps to evaluate affiliates' readiness. *(DOS)*

SBA Establishes End-user Review and Validation Groups Per OIG Recommendations

Starting in March 1998 and continuing through December 1999, the Small Business Administration (SBA) OIG and SETA, a technical consulting firm, conducted "independent verification and validation" of SBA's efforts to ensure that its information systems would function properly in the Year 2000 and beyond. Using guidance provided by GAO, they evaluated SBA's efforts in terms of awareness, assessment, renovation, validation, and implementation.

Throughout the project, the OIG and SETA issued progress and assessment reports. In July 1999, SETA concluded that SBA was basically Y2K compliant, but stressed the need for end-user participation and review of systems integration testing. Because this was a critical sub-phase for ensuring Y2K compliance, the OIG issued an advisory report formally recommending end-user involvement in system integration and acceptance testing. As a result, SBA's CIO and SBA program offices established end-user review and validation groups. SETA and the OIG continued their efforts through the remainder of 1999, working closely with the end-user groups in reviewing test plans and scenarios, input data, output results, comparison test runs, errors, and corrective actions, to certify the Y2K readiness of all SBA mission-critical systems. *(SBA)*

Audit Identifies Areas of Improvement to Ensure VA's Y2K Compliance

The Department of Veterans Affairs (VA) OIG assessed VA's efforts to address computing issues and become Y2K compliant. The review found that VA organized its efforts well and focused them on its mission-critical systems. VA management reports showed that it completed implementation of all mission critical systems by the March 31, 1999 milestone date established for all federal agencies.

The audit identified issues that could help make overall efforts more successful, reduce operating costs, and ensure continuity of operations. Key areas that VA needed to address included: 1) infrastructure support, 2) contingency planning, 3) assuring that computers, biomedical devices, and equipment provided for home use were Y2K compliant, and 4) approval of pending requests for equipment and software replacements that would reduce operating costs by $1.5 million and enhance implementation efforts. Because of the high risk associated with failure to comply, OIG recommended that VA continue to monitor Y2K risk as a potential material weakness area. *(VA)*

SSA Takes Action to Address OIG Concerns on Y2K Compliance

The Social Security Administration (SSA) OIG conducted an audit to determine whether SSA's non-mission-critical software had been identified and validated for Y2K compliance. The review identified two areas of concern. First, SSA's Y2K inventory of non-mission-critical software was incomplete. Without a complete Y2K inventory maintained on SSA's servers, SSA could not ensure that all of its commercial software was Y2K compliant. Second, OIG tests identified 54 data files (32 percent) provided by commercial applications with two-digit dates. Files having two-digit dates could potentially disrupt SSA's non-mission-critical operations with system failures or corrupt information.. *(SSA)*

OIG Audits Assess Readiness of Treasury's Critical, Computer-dependent Operations

One of the most significant concerns in the area of information technology during FY 1999 was the effect which the century date change, or Y2K, would have on Department of the Treasury systems. Y2K had the potential to affect virtually every aspect of Treasury operations, since virtually all its functions rely to some degree on automated computer processes.

The OIG conducted numerous audits of Treasury's efforts to ensure its systems, applications, and infrastructures were compliant. In an August 1999 summary report, the OIG recommended strengthening Treasury's compliance process, thereby reducing its Y2K risk. The OIG also reviewed Treasury's oversight efforts towards ensuring effective compliance testing and contingency planning for business continuity. *(Treasury)*

OIG Advises Education to Monitor Y2K Readiness of Trading Partners

The Department of Education (ED) OIG conducted reviews of Year 2000 readiness at selected ED trading partners and communicated the results to the department to assist in its development of contingency plans. The OIG completed reviews at 10 guaranty agencies and one public school district during FY 1999. OIG auditors found the progress at five of these entities to be satisfactory, except for one guaranty agency assessed as cautionary. Issues identified at some of these agencies were similar to those facing the department as a whole: 1) data exchanges, 2) contingency planning, and 3) risks associated with new systems.

OIG's subsequent review of Y2K readiness at six guaranty agencies identified three issues the department needed to address as it continued to monitor the 36 guaranty agencies participating in the Federal Family Education Loan Program. First, entities could receive erroneous data or no data if one or more of their data exchange/trading partners had computer failures. These failures could make the entities incapable of performing their functions effectively. Second, five of the six agencies had not established Y2K contingency plans, although three of the five had plans to do so. Third, OIG advised the department it needed to actively monitor guaranty agencies that implement new systems in 1999. *(ED)*

OIG Finds All Systems Y2-OK for Amtrak

In October 1996, Amtrak initiated a major initiative to renovate its information systems and achieve Y2K readiness. The OIG performed an interim review in September 1998 and a subsequent follow-up assessment in FY 1999. The OIG noted that all mainframe computers and operating systems were Y2K ready and that Amtrak's reservation and ticketing system (Arrow) was already providing Year 2000 reservations and ticketing. Almost all business applications were renovated, and virtually all data/voice networks, the Internet booking site, and most mid-range and personal computer systems were ready. All major suppliers of power and a majority of fuel vendors had indicated Y2K readiness. Amtrak received more than an 80 percent response rate to Y2K questionnaires it sent to key business partners and suppliers. Amtrak also performed a legal review of several contracts with key information technology vendors and commuter/state authorities. OIG recommended that the main focus of Amtrak's efforts for the remaining few weeks to the Y2K deadline be contingency planning. *(Amtrak)*

Board of Governors Responsive to OIG Recommendations on Century Date Change

During 1999, the Federal Reserve Board (FRB) OIG continued to monitor the Federal Reserve System's (FRS) Board of Governors' (Board) century date change (CDC) efforts. These efforts aimed at ensuring the readiness of supervised banking institutions, remediation of the Board's internal operations, and oversight of preparations by FRS operations and payment systems. The OIG focused increased attention on Board and FRS event-management initiatives to address risks of potential disruptions at the century rollover. Board management and staff were quick to address issues and concerns that OIG raised and, where necessary, made appropriate adjustments to CDC programs. *(FRB)*

OIG Questionnaires Assess Y2K Readiness of NEH

By using various questionnaires, the National Endowment for the Humanities (NEH) OIG found that NEH was not going to implement the new relational base grants management system and the new off- the-shelf accounting system. The OIG then monitored NEH's Y2K patch for the WANG and Microsoft software used on its secondary system. The OIG also had NEH prepare a Day 1 plan. *(NEH)*

OIG Assesses NLRB Progress in Making Systems Y2K Compliant

The OIG evaluated the National Labor Relations Board's (NLRB) efforts in identifying Y2K problems and actions taken or planned to ensure that mission-critical systems would function in the new millennium. NLRB identified 33 mission-critical systems, and the OIG verified that software for 20 of the 33 was compliant. Agency officials reported that seven systems were made compliant after audit fieldwork was completed, and five more were completed by March 31, 1999. The Financial Management Information Accounting System (FMIAS) was compliant by May 1999.

FMIAS is NLRB's accounting system, which it uses to process and report budget and financial transactions. Actions needed to bring FMIAS into compliance included upgrading its compiler and changing the source code of several program modules. NLRB's contingency plan included using one of two other accounting systems, both Y2K compliant, to process vendor payments. Agency-wide compliance was contingent on making applicable computer hardware Y2K compliant. The OIG reviewed NLRB's action plan to upgrade hardware and finish programming remaining systems, and concluded that their goal was attainable. *(NLRB)*

NARA Begins Implementing OIG Recommendations to Make Systems Y2K Compliant

The National Archives and Records Administration (NARA) OIG reviewed NARA's efforts to address the Year 2000 problem. The OIG found that: 1) the estimated completion date for renovating the NARA network (NARANET), a mission-critical system, slipped from June 1999 to August 1999, leaving only four months for testing and operating the renovated system; 2) there were no estimated completion dates for 17 of 36 buildings leased from the General Services Administration (GSA), and NARA officials were not monitoring the Y2K status of the facilities; 3) fixes for the non-mission-critical systems may not be completed by the OMB target date; and 4) NARA had not prepared a business continuity and contingency plan, nor had senior management officials participated in the business continuity and contingency planning effort.

The OIG recommended that NARA: 1) provide technical assistance to program offices, by identifying non-mission-critical systems that are not Y2K compliant and make them compliant; and 2) review the status of GSA's compliance efforts and whether level IV&V testing has been accomplished for leased buildings. In addition, the OIG recommended that if field offices cannot obtain the required information to determine the Y2K status of buildings leased from GSA, management should require them to: a) determine if the Y2K-compliant systems have been tested, and b) obtain estimated completion dates for those buildings which have systems that are not Y2K compliant. Management concurred with OIG's findings and initiated actions to begin addressing the concerns. *(NARA)*

OIG Suggests Actions to Improve NCUA Follow-up in Waiver Process

The National Credit Unio n Administration (NCUA) OIG conducted a review to evaluate NCUA's efforts in monitoring and assisting federally insured credit unions to address Y2K date compliance through the waiver process. NCUA had established a policy in early1998 of providing waivers or extensions to credit unions regarding the milestone dates in specific instances, such as converting from one information system to another, or when credit unions lacked the ability to meet the milestone dates because of system renovation. NCUA granted waivers and extensions for individual credit unions and blanket waivers for some credit unions with common information system vendors. The overall objective of the OIG review was to evaluate the success of NCUA's monitoring and assistance efforts.

The OIG observed that: 1) waiver actions were justified; 2) there was a lack of documented follow-up actions; 3) the waiver process was lengthy; and 4) additional attention was needed for federally insured state chartered credit unions. The OIG offered a number of suggested actions as matters for consideration by the NCUA Board and agency management. *(NCUA)*

OIG Actively Monitors NSF's Progress in Ensuring Y2K Compliance

The National Science Foundation (NSF) OIG took important steps during FY 1999 to monitor NSF's efforts to ensure Y2K compliance. The OIG participated in NSF's selection of a contractor to perform an independent verification and validation of its progress toward Y2K readiness. The OIG also reviewed NSF's quarterly progress reports to OMB and periodically met with GAO, which monitored each agency's progress in becoming Y2K compliant. At NSF's request, the OIG observed its contractor's testing of systems to understand and assess the overall reasonableness of the methodology and procedures used to obtain test results. NSF reported all mission-critical systems Y2K compliant, and although the OIG did not independently test NSF's systems, it expressed satisfaction, based on its review of work performed by NSF's outside contractor, that NSF had taken all reasonable steps to ensure that its systems were compliant. The OIG also participated in a test that simulated processing during the Year 2000 on smaller systems developed for specific NSF offices. *(NSF)*

OIG Recommends Y2K Contingency Plan to Ensure Continuity of Maritime Operations

An OIG review disclosed that the Panama Canal Commission (PCC) had not prepared a Y2K contingency plan for the Marine Traffic Control (MTC) system in time for completion of Build 1 of the Enhanced Vessel Traffic Management System (EVTMS) project. Build 1of the EVTMS project was initially scheduled for completion in November 1998. The project itself, which was intended to replace the existing Marine Traffic Control (MTC) system and solve its Y2K software problem, was running about nine months behind schedule at the end of the fiscal year.

The OIG recommended that PCC management prepare a Y2K contingency plan. As a result of the OIG recommendation, the EVTMS project personnel prepared a Y2K contingency plan for the MTC system to ensure continuity of maritime operations. *(PCC)*

USPS Makes Significant Progress Toward Y2K Preparedness with OIG Partnership

In February 1999, the U.S. Postal Service (USPS) IG testified before the House Subcommittee on the Postal Service regarding the major Y2K challenges facing USPS. She expressed concern that USPS had neither comprehensive postal-wide planning nor sufficient senior management involvement to allow for the most effective approach to managing the Y2K problem. Based on OIG audits completed at that time, mainframe operating systems were not entirely compliant; critical information systems were not correctly identified, prioritized, or tested for compliance; and status reporting was not always accurate.

Since then, the OIG completed eight additional audits addressing USPS external suppliers, mail-processing equipment, and facilities, the operations of which are technology-driven; information systems; and business contingency and continuity planning. By engaging management early and frequently during these audits and partnering with postal managers in critical areas, the OIG was able to help the USPS work more productively toward achieving the common goal of Y2K preparedness. As a result of management's responsiveness to OIG recommendations and their commitment to this effort, the USPS made significant progress in preparing for Y2K. *(USPS)*

OIG Finds SEC Took Numerous Steps to Address Y2K Issues

As part of an ongoing Year 2000 audit, the Securities and Exchange Commission (SEC) OIG issued two reports during FY 1999 on SEC's Y2K compliance efforts. One covered internal SEC systems, while the other covered EDGAR, SEC's most important system that disseminates financial information to investors.

The OIG found that SEC had taken numerous steps to address the Y2K issue. These included intensified senior management involvement, enhanced project tracking and planning, and development of test plans. The OIG recommended that management support the Year 2000 project separately from a reorganization in the Office of Information Technology (OIT), thereby enhancing OIT's decision-making processes, and prepare a final EDGAR test plan. *(SEC)*

Comprehensive OIG Review Yields Suggestions for Improvement in FCC's Y2K Program

The Federal Communications Commission (FCC) OIG initiated a comprehensive program to review the FCC preparations to prevent a possible disruption of service as a result of Y2K anomalies. The two goals of this program were to provide the FCC Commissioners with an independent assessment of the Commission's Y2K efforts and to recommend improvements to its readiness program. To meet these goals, the OIG reviewed FCC's Year 2000 program, including its efforts in system remediation, application testing for Y2K compliance, business continuity and contingency planning, and Day-One strategy development. OIG provided the Commission with both an objective review of FCC's Y2K program and with concrete suggestions for its improvement. *(FCC)*

ITC Establishes Y2K Committee to Carry Out OIG's Recommendations

The International Trade Commission (ITC) OIG submitted an audit report on ITC's Y2K readiness. The report concluded that the Commission would likely experience some disruption because of the Y2K problem. The OIG recommended that the Chairman appoint an official to: 1) manage the Commission's Y2K activities, 2) identify all systems, 3) assemble a team to coordinate Commission efforts, 4) develop a Y2K policy action plan, 5) increase awareness of the Y2K problem, and 6) provide technical training.

As a result of those findings, the Chairman designated the director of operations as the official to oversee ITC's Y2K preparation efforts. The director assembled a Y2K Committee that reported to the Commission biweekly on progress. Additionally, the Commission and OIG concluded that it would be beneficial to do periodic reviews of the Commission's Y2K activities. *(ITC)*

OIG Monitoring Efforts Find FLRA Fully Y2K Compliant

The Federal Labor Relations Authority (FLRA) OIG continuously monitored FLRA's Y2K progress throughout FY 1999. Since early funding estimates for Y2K compliance activities were low because assessments of Y2K needs were not completed and hard data was unavailable for budget programming for FY 1999, the FLRA had to request additional supplemental Y2K funding. The FLRA was one of six federal agencies receiving Y2K supplemental appropriations, and set up a specific accounting system for Y2K expenditures to track supplemental appropriated spending.

The OIG found that all of FLRA's mission-critical systems were either repaired or replaced during FY 1999, to be fully Y2K compliant. The FLRA's Information Resource Management staff advised the OIG that it planned to spend the remainder of the calendar year testing the hardware and software to ensure maximum utility. In addition, the FLRA developed a Year 2000 remediation plan to ensure that its automated systems would function properly beginning January 2000. *(FLRA)*

OIG Focuses on System Validation and Implementation in Evaluating EEOC Readiness

The Equal Employment Opportunity Commission (EEOC) OIG actively evaluated the agency's efforts in information technology development and implementation during FY 1999. The OIG provided assistance in an oversight capacity to the EEOC as it sought to ensure Y2K compliance of all its mission-critical and non-mission-critical systems. The OIG concentrated its efforts during FY 1999 on system validation and implementation to ensure total system compliance prior to December 31, 1999. Furthermore, the OIG performed a review of EEOC's various contingency plans and Day-One Plan to ensure their adequacy in addressing any Y2K concerns. *(EEOC)*

Independent OIG Reviews Find Documentary Support for Closed Mission-critical Items

During FY 1999, the Tennessee Valley Authority (TVA) OIG participated on a team that selected a consultant to perform an external assessment of TVA's Year 2000 program. Based on the results of the consultant's assessment, the OIG decided to perform independent reviews to determine if 1) mission-critical items reported as closed were supported by appropriate closure documentation, and 2) continuity plans supported operational readiness and safety. Two subsequent audits found mission-critical items reported as closed were supported by documentation. Three OIG audits of TVA's Y2K continuity plans were in progress at the end of the fiscal year. *(TVA)*

OIG Engages in Year-long Effort to Monitor Agency's Y2K Compliance

The OIG at the Federal Maritime Commission (FMC) periodically reviewed the agency's readiness to ensure an orderly transition to the Year 2000. Management furnished periodic reports on Y2K progress to the OIG during the year, which OIG reviewed. Overall, the OIG found FMC's critical systems Y2K compliant. *(FMC)*

B. Helping Promote Systems Security: Audit Activities

One of the most critical mandates for information-system managers is to ensure systems integrity. IGs have an important role in identifying potential as well as existing problems, both one-time and systemic. In so doing, IGs perform an indispensable role in helping ensure the integrity of their agencies' information systems, and that of their programs.

In FY 1999, IGs performed important work across the board in the area of systems security, as shown below.

DoD Audits Highlight Recurring Security Management Problems

DoD OIG published a January 1999 summary report that provided a comprehensive assessment of systems security vulnerabilities, as indicated by 75 previous audit reports from various sources. It also issued seven additional reports during FY 1999 that addressed information assurance. Cumulatively, this body of work indicated widespread problems related to access control, database audit trails, policies and procedures, system certification and accreditation, training, contingency planning, separation of duties, delineation of responsibilities, risk analysis, and other aspects of security management for DoD's 10,000 networks and 1.5 million computers.

The summary report was particularly useful in emphasizing the recurring nature of audit findings and the need for more innovative and lasting solutions to long-standing vulnerabilities. The report also illustrated the audit community's capability to support management through a wide-range of services from assessments of departmental policy to on-site security audits of systems and processing centers. *(DoD)*

OIG Finds Spotty Computer Security Policy Implementation at DOJ

DOJ OIG completed an audit of an automated system that its law enforcement agencies jointly operated and used. The audit found that computer security controls, including password management and intruder lockout protection, were not in place to protect the system and sensitive data from unauthorized use, loss, or modification. The DOJ OIG recommended that DOJ adhere to and monitor compliance with existing policy and develop and implement new policy to address the weaknesses. DOJ has taken steps to address these weaknesses. *(DOJ)*

HUD Makes Slow Progress in Correcting Systems Security Weaknesses

HUD's automated information systems are critical in supporting all facets of its programs, mortgage insurance, servicing, and administrative operations. The OIG reviews HUD's systems security as part of its financial statements audit. As in prior years, systems security weaknesses continue to exist. These weaknesses include general system controls and controls over certain applications, as well as weak security management. These controls are important to protect data, funds, property, and assets from waste, loss, unauthorized use or misappropriation. While HUD plans to correct the weaknesses and has made some security improvements, implementation progress has been slow. *(HUD)*

OIG Review Leads to Prosecutions for Unauthorized Use of Long-distance Telecommunications at GSA

An OIG proactive review of computerized telecommunications switches maintained by GSA uncovered voice-mail system vulnerabilities. These vulnerabilities, which permitted unauthorized individuals to access long-distance telecommunications via the voice-mail system, were resulting in losses of up to $100,000 per incident. As a result of the OIG review, the OIG joined a task force with the U.S. Secret Service and the Federal Bureau of Investigation to investigate computerized intrusions and use of access devices. During FY 1999, the task force has served 16 search warrants leading to six arrests/indictments and two convictions. The task force continues to expand its efforts into illegal intrusions of computerized telecommunications systems. *(GSA)*

OIG Recommends Improved Security Management at DOL

Over the course of three months, the Bureau of Labor Statistics (BLS) experienced three information technology system security breaches. The three incidents included two inadvertent premature releases of sensitive economic data, and an intruder defacing BLS's web page. The early release of sensitive economic data can affect financial markets. DOL OIG's audit efforts focused on physical and automated security practices and procedures in three specific areas: information technology, program survey offices, and administration.

In general, the OIG found that BLS operated and managed these three areas without benefit of sound internal controls, and that pervasive problems existed in BLS' internal control structures. The audit report contained 41 recommendations, which when implemented should eliminate or mitigate the audit findings. *(DOL)*

OIG Report Finds Contractor-implemented Controls Inadequate for OPM System

OPM OIG evaluated the general controls environment of a Federal Employees' Health Benefit Program (FEHBP) contractor's computer system. The goal was to obtain reasonable assurance that the contractor implemented proper controls over the integrity, confidentiality, and availability of computerized data associated with the processing of FEHBP health benefit claims and the accurate reporting of costs to OPM. The auditors found weaknesses in the contractor's mainframe security software and application-based security profiles. As a result, there is an increased risk that someone could gain unauthorized access to the contractor's computer system. In total, OIG issued 22 recommendations intended to improve logical and physical access controls, controls over software development and changes, systems software, and disaster recovery. The contractor agreed with OIG's recommendations and began implementing them. *(OPM)*

Computer Security Planning and Management Need Strengthening at USDA

USDA OIG found that a major computer center needed to strengthen its process over the management and planning of computer security controls. The review disclosed vulnerabilities in the center's computer network, the lack of a network-monitoring and intrusion-detection program, and access authority not appropriately limited for authorized users. The vulnerabilities identified in the computer network, if left uncorrected, could allow unauthorized internal or external users to gain access to data, allow unauthorized users to modify or destroy the data, or cause service disruptions. Without the proper controls, the center has reduced assurance that unauthorized access to systems on its network would be detected in time to prevent or minimize damage. OIG also found that the center needed to strengthen controls over identification numbers (ID) and passwords; otherwise, sensitive financial information is at increased risk of unauthorized modification or disclosure. In addition, insufficient actions had been taken to implement and/or enforce the critical security requirement that Privacy Act or sensitive data such as computer ID's and passwords be encrypted if sent over the Internet. *(USDA*)

OIG Recommends Improvements in Securing Housing Taxpayer Information at IRS

Virtually all IRS transactions affecting a taxpayer's account are processed through Unisys computers. They house databases for on-line retrieval of taxpayer information; therefore, it is critical for these systems to have an effective general controls environment. TIGTA OIG reviewed the general controls over IRS' Unisys 2200 Operating System environment and concluded they are adequate to protect sensitive data. However, there are several areas where the IRS could adhere to controls more uniformly, and should establish procedures to provide improved system control, security, and standardization.

The OIG recommended several ways to improve controls over taxpayer data files and the common system and database files. In addition, the auditors recommended: 1) modification of control settings for files that may potentially complicate the mainframe consolidation process; 2) development of a process to improve accountability of individuals using the system-security user identification; 3) re-issuance of the policy for accounting for deviations of user access profiles from IRS standards; and 4) development of C2-level security documentation, security policies, and documentation of risk factors for the Unisys consolidated mainframe environment. *(TIGTA)*

Comprehensive Reviews of DOC Information Management Systems Prompt Action to Strengthen Security

During FY 1999, DOC OIG performed comprehensive reviews of information management systems security in support of annual financial statement audits. Conducted at DOC's major information technology data centers, and based on GAO's *Federal Information System Controls Audit Manual*, the reviews assessed whether: 1) overall entity-wide security program planning and management was effective, 2) access controls were adequate, 3) application software development and change control was effective (as related to financial management information systems), 4) system software controls were adequate, 5) duties of key operational aspects were properly segregated, and 6) service continuity plans were comprehensive (backup, recovery, and contingency planning). The OIG also conducted a comprehensive network analysis (i.e., penetration testing) at one of the major information technology processing centers to assess both internal and external vulnerabilities. In response, DOC information technology managers are taking prompt action to strengthen security. *(DOC)*

OIG Recommends Improvements to USPS Computer Monitoring and Security Policies

USPS OIG issued a management advisory to USPS management recommending improvements to its policy regarding monitoring computer systems and computer warning banners. OIG recommended that USPS place standardized warning banners on all its computers and networks, alerting users that any use of a computer was subject to monitoring. The OIG also recommended that USPS amend its computer security policy to specifically authorize managers to monitor employees' use of computers. Management agreed with the recommendations, and agreed to implement them. *(USPS)*

OIG Works with ED Managers to Resolve Security Findings

ED's Grants Administration and Payment System (GAPS) is a core component of its Central Automated Processing System. The OIG worked with the Department during FY 1999, resolving all but one of the 45 GAPS system security findings reported in a September 1998 review. The review, an assessment of the overall security surrounding GAPS production environment, identified a number of technical and procedural security exposures. The OIG's recommendations presented opportunities for the enhancement of GAPS security in the areas of security access control, security option settings, audit trail controls, cash management, security administration, ensuring accountability, and appropriate segregation of developers from security and application functions. *(ED)*

OIG Finds Previously Identified Problems Remain at HHS

As part of its audit of the Department's financial statements, the HHS OIG reviewed general and application controls at the Health Care Financing Administration (HCFA). Although the review identified no new material weaknesses, the OIG found that previously identified control problems persist as implementation of much of HCFA's corrective action is scheduled for future FYs. The review identified weaknesses in several of the claims-processing system applications that could result in improper payment of Medicare claims; access to source code, which could result in implementation of unauthorized programs; and weaknesses that would result in inappropriate override of certain standard programs.

As part of OIG's overall responsibility for the protection of the Department's programs from criminal activity, the Office of Investigations has also taken steps to initiate a new Computer Intrusion Unit, which will investigate crimes that target HHS computers. *(HHS)*

OIG Recommends Agency-wide Information Systems Security Program at SBA

An audit of SBA's general information systems controls, which incorporated GAO's *Federal Information Systems Control Audit Manual*, revealed that SBA's general controls were not fully compliant with established policies and procedures. The auditors found: 1) SBA had not funded and implemented an entity-wide security program; 2) unnecessary and excessive access privileges reduced accountability and created segregation-of-duties weaknesses; 3) application-development and change-control procedures were not consistently applied in systems outside OCIO's control; 4) programmers' abilities to access operating systems could not be monitored; and 5) security administrators and program managers needed training.

The report recommended the establishment of an agency-wide, information systems security program, and a committee to address the audit findings. SBA management concurred with the recommendations, and identified both financial and human resources to develop solutions and implement procedures to resolve these outstanding issues. *(SBA)*

OIG Identifies Weaknesses in Amtrak's Safety Information System Control Environment

Amtrak's OIG performed a review of Amtrak's Safety Information System, which is a client-server application with on-line processing and a centralized database. Amtrak uses this application system for federal reporting requirements and as a decision support tool for management.

The OIG observed several weaknesses in the control environment of the Safety Information System. It noted that a disaster recovery plan was not developed and regularly scheduled drills were not performed. Additionally, the OIG determined that once application level passwords were assigned, they never expired. Furthermore, system user lists were not up to date, anti-virus programs were not installed, and certain roles and responsibilities were not properly segregated. The OIG recommended strengthening the general and application controls for the Safety Reporting System. *(Amtrak)*

OIG Notes Weaknesses in Security Management of GPO's Information Systems

The Government Printing Office (GPO) OIG issued an audit report that assessed the adequacy and effectiveness of the Office of Information Resources Management (OIRM) management control program. The OIRM provides information resources management services to GPO, other federal agencies, and private individuals. OIRM performs feasibility studies to determine the need for GPO-wide information systems and programs. OIRM also designs, develops, and maintains agency data processing, office automation, local and wide area networks, and telecommunications systems.

The audit noted that as of February 1999, OIRM had identified and completed self-assessments of six major areas involving 81 controls. While OIRM attempted to identify, assess, and test its internal controls, the work was incomplete. Of the 42 high-level controls the OIG identified in its application of a leading comprehensive methodology, OIRM addressed relatively few. The OIG recommended that OIRM's director strengthen internal controls over: 1) completing accurate self-assessments with documentation; 2) implementing and resolving open audit recommendations; 3) testing software program changes; 4) authorizing access to the computer system; 5) developing and maintaining collective and individual training plans; and 6) keeping only used systems software in the mainframe. *(GPO)*

OIG Review Results in Better Management of PCC Client-server Security

PCC has incorporated client-server systems into its overall information technology network. These systems require a sound security program to prevent unauthorized access and intrusions to obtain sensitive information, commit fraud, or disrupt operations. The OIG review disclosed that security controls established in PCC's client-server environment were not effectively managed, and were inadequate to ensure the integrity, confidentiality, and availability of information and systems.

PCC management took several actions to address the weaknesses. First, management developed guidelines for restricting remote access to networks and enhancing and fortifying security administration;. Second, it controlled the number of employees who were granted rights to administer corporate servers. Third, it modified the format of default passwords given to new users. Fourth, it maintained an audit trail of the functions which system programmers and database administrators performed, and instructed PCC's information security officer to monitor these trails on a regular basis. *(PCC)*

OIG Identifies Areas for Improvement in TVA Computer Security

TVA OIG audited security and access controls for TVA servers, sensitive information on TVA's Intranet and Internet sites, and non-TVA personnel in TVA's electronic mail system. The objective was to ensure that adequate security and access controls were in place to protect TVA systems and information from unauthorized access.

The review identified opportunities for improvement in security: 1) for all servers, and 2) in the access to sensitive information through TVA's intranet by non-TVA employees. During the audit, OIG identified opportunities for improvement in the areas of 1) compliance with TVA's security manual; 2) guidance given to owners of information available through the system; and 3) implementation of TVA procedures. *(TVA)*

OIG Recommends Improvements to Protect FEC Information Systems from Disruptions

In September 1998, the Federal Election Commission (FEC) OIG began an audit of FEC's management of computer software. The audit objectives were to: 1) verify that FEC's computer software was in compliance with applicable copyright laws, and FEC policies and procedures on software use; 2) determine that adequate policies and procedures were in place to prevent unauthorized software use by FEC employees; and 3) ensure that adequate controls were in place to detect and prevent computer viruses.

The OIG concluded that controls should be strengthened to ensure that FEC computers are adequately protected from computer viruses. The OIG provided several recommendations to FEC management to improve the protection of computers from potential disruption and damage caused by viruses. The audit report also included a suggestion that management develop an adequate record-keeping system to ensure that all software complies with copyright laws. FEC management was receptive to the recommendations and began to implement them subsequent to the audit. *(FEC)*

OIG Finds Security Management of Bureau of Indian Affairs' Automated Systems Inadequate

As part of a follow-up audit on recommendations pertaining to general controls over automated information systems contained in two prior Bureau of Indian Affairs' (BIA) audits, the DOI OIG found that only three of the 20 recommendations had been fully implemented. General controls over BIA's automated systems were ineffective in its security program, access controls, software development and change controls, segregation of duties, and continuity of service. As a result, BIA is at risk of loss, misuse, modification of, or unauthorized access to the data in its automated information systems.

The OIG noted deficiencies in three key areas. Controls over computer access and physical access to computer facilities were inadequate to ensure that only authorized users had access to data. Further, configuration management (changes to programs, data, and documentation) controls were inadequate and did not ensure segregation of duties, while documentation for three mission-critical systems had not been maintained for more than 10 years. Finally, information technology systems security had not been instituted because BIA had not performed security reviews of its automated systems, developed security plans for major applications and general support systems, or developed adequate contingency plans. While BIA has developed a plan to correct these deficiencies, the OIG continues to cite general controls over its automated information systems as a material internal control weakness. *(DOI)*

OIG Identifies Areas for Improvement in FCA's Network Infrastructure

The Farm Credit Administration (FCA) OIG assessed FCA's network infrastructure. The OIG focused its analysis on business process improvement; current network infrastructure design; network monitoring tools used to manage and monitor the network; staffing levels and organization; network security policies and procedures; and whether the infrastructure could support future initiatives.

The OIG found the network infrastructure well designed and documented with technology comparable to or better than other information technology organizations throughout industry and government. FCA has acquired top-of-the-line equipment from leading vendors that will provide it with a robust infrastructure for the foreseeable future. Nevertheless, the OIG identified areas for improvement and offered 20 recommendations to address them. *(FCA)*

OIG Finds SEC's Security Practices Reasonably Effective

SEC OIG evaluated the Commission's security practices over its Unix systems at the data center in Alexandria, Virginia. The audit found that security practices were for the most part reasonably effective.

Some general issues (including user training, password use, and written procedures) will be addressed as part of the Commission's overall effort to improve computer security. The OIG made several specific recommendations to enhance Unix security practices, including updating network maps and periodically changing and validating root passwords. *(SEC)*

OIG Review Discloses Deficiencies in SSA Contingency Planning Program

SSA OIG conducted an audit to follow up on prior audit findings related to SSA's backup and recovery procedures. The OIG expanded its scope to address the overall effectiveness of SSA's contingency planning for unexpected events that could interrupt service delivery throughout its operations. Inadequate contingencies preparation could significantly impact SSA's ability to provide timely customer service.

The OIG found that SSA's contingency planning program did not comply with federal criteria established by the Computer Security Act of 1987, OMB Circular A-130, *Security of Federal Automated Information Resources*, and the National Institute of Standards and Technology. The OIG attributed the fundamental cause of the deficiencies it identified to an infrastructure that lacked clearly defined roles and responsibilities for contingency planning. The report contained 20 recommendations, with which SSA in general agreed. SSA officials advised the OIG that they had convened an agency-wide task force to address contingency-planning issues. *(SSA)*

OIG Identifies Deficiencies in Customs Service's Ability to Restore Critical Systems

The need for adequate security to protect data from unauthorized access and to ensure the reliability of computerized data is critical for the Department of the Treasury and the federal government as a whole. Automated systems security continues to be an important issue for the Treasury. This year, in its report on the U.S. Customs Service's FY 1998 financial statements, the OIG identified deficiencies in Customs' ability to provide for timely restoration of mission-critical systems. The OIG issued a follow-up report that detailed the significant operational impact that could result from deficiencies in Customs' disaster recovery capability and other data security weaknesses. *(Treasury)*

OIG Works with FRB Staff on Business Continuity and Contingency Plans

To accomplish Y2K oversight activities, the FRB OIG worked with Board staff across divisions and offices to ensure consistency and coordination of application testing, business continuity and contingency planning, and event management planning. The OIG completed test documentation reviews of 141 medium-critical applications and provided guidance in resolving discrepancies. The OIG also coordinated with an external consultant on a more detailed review of the Board's 16 mission-critical applications. The OIG's assessment of the business continuity and contingency plans stressed the need to perform validation testing. *(FRB)*

OIG Penetration Testing Highlights Problem Areas in DOE

DOE OIG performed penetration and vulnerability testing at a number of sites during FY 1999. The recently formed Technology Audit Group performed the testing, with assistance from contractor computer-security experts. Group members utilized both commercial and publicly available software to evaluate security protecting financial-related networks. Testing revealed significant internal and/or external weaknesses that rendered the DOE's unclassified computer networks vulnerable to malicious attack by either internal or external parties. Internal network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, and/or outdated software with known security problems were observed on a number of networks. External vulnerabilities associated with firewall configuration and many of the same problems noted during internal network testing were also observed. *(DOE)*

NEH to Implement New Systems and Transactions

NEH OIG learned that the NEH had no significant plans to implement additional security this year, but will be using an accounting system and a new grants management system. In addition, NEH expects to implement some Internet-based transactions with grantees. The OIG is working with NEH to find an acceptable position. *(NEH)*

OIG Plans to Use Penetration Test Results to Improve NSF's Automated Systems

NSF OIG expanded the audit scope of NSF's FY 1999 financial statements to include a more comprehensive review of NSF's data processing systems and its internal computer network. The OIG tested for compliance with all of the controls in GAO's *Federal Information System*

Controls Audit Manual. As an additional part of this review, the OIG contracted with industry experts to perform penetration tests to identify and expose vulnerabilities in NSF's data processing system. The main purpose of this testing was to evaluate the overall data processing environment, and in particular, the critical financial systems, and assess their vulnerability to unauthorized access and use. The OIG will use what it learned from this specialized testing to improve the security of NSF's automated systems. *(NSF)*

ITC Implements OIG Suggestions to Improve *Passport* System's Security

ITC OIG conducted a review of the ITC's *Passport* system, a new remote-access facility that ITC introduced in August 1998. The objective was to evaluate the *Passport* system's security and identify potential security risks. Within the limited parameters of this evaluation, the OIG was unable to penetrate into the *Passport* system or the system it protects. However, the OIG identified certain vulnerabilities that could potentially be exploited to obtain access.

The OIG suggested that the Director of Information Services disable system services, prevent the download of certain files, and remove an option for mail service from a non-mail server. The Director of Information Services implemented the recommendations. *(ITC)*

Multidisciplinary Team Identifies Security Vulnerabilities at FCC

FCC OIG created a multidisciplinary team to respond to a report that a major mission-critical computer system had been externally attacked. Using computer forensic techniques, the OIG investigated this incident and determined that the system had not been penetrated. In fact, the review team was able to demonstrate that the security incident actually resulted from a feature of the database management system being used and that the security boundary was configured correctly.

As part of the response, the review team employed sophisticated network analysis techniques to analyze 28 Unix systems and other devices, such as routers, to assess the organization's overall computer security posture. The analysis used an advanced automated investigative tool that can identify such serious security vulnerabilities as user accounts without passwords and system files with world-writeable access. The review team identified 44 findings and is working with Commission staff to enhance computer security by implementing the recommendations. *(FCC)*

OIG Review Prompts Security Enhancements of FTC Automated Information Systems

An OIG review of aspects of the Federal Trade Commission's (FTC) automated information management program resulted in enhanced security of automated information resources and improvements in overall system efficiency. The OIG performed a penetration test of the agency's computer system that involved 1) external probes via the Internet to the agency's firewall; 2) external probes though dial-in modems; and 3) internal probes of the network from within the FTC. The OIG was able to penetrate the agency's internal network in the same way that a "hacker" would likely attempt to access the network. OIG also identified (and provided management) step-by-step "hacking" instructions freely available on the Internet that would enable an individual with some sophistication to exploit many of the vulnerabilities the review identified. Responding to OIG's findings, management disconnected unused modems, changed system default passwords, and appointed a security officer to monitor these and other vulnerabilities. *(FTC)*

C. Inspections or Other Analytical Work in Systems Security

Inspections or other work in systems security involve the identification of anomalous computer activity using data analysis tools, e.g., periodically analyzing computer logs for suspicious log-in attempts.

OIG Recommends Improvements to NASA's Incident Response Capability

NASA relies on state-of-the-art computers, and on local- and wide-area networks to perform critical missions and conduct business operations. NASA networks, however, can be compromised for unauthorized and/or malicious purposes. To combat this, in 1993 NASA established its Automated Systems Incident Response Capability (NASIRC) as a result of increasing attacks against its computer systems and networks.

The OIG examined NASA's capability to respond to incidents and attacks involving its automated information and telecommunications systems. The report addressed the adequacy of NASA's incident reporting, response, handling, coordination, and information-sharing capabilities. While NASA has taken many positive steps to enhance computer security and its response to information technology attacks, NASA needs to take additional actions to fully address increasing threats, including clearly delineating NASIRC's roles and responsibilities. NASA management concurred with the report's 11 recommendations. *(NASA)*

DoD OIG Launches Two New Investigative Sections

DoD has taken an aggressive stand to protect the DoD infrastructure against both internal and external cyber intrusions. As part of this aggressive approach, the Defense Criminal Investigative Service (DCIS), the criminal investigative arm of the OIG, DoD, has incorporated two new sections into their arsenal of investigative tools. They are the Defense Information Infrastructure Intrusions Investigative Team (DI4T) and the Seized Computer Evidence Recovery Specialists (SCERS).

The DI4T provides immediate criminal investigative response to suspected computer intrusions. The DI4T also develops and disseminates criminal intelligence to assist in protecting the Defense Information Infrastructure (DII), coordinates and conducts liaison with DoD and other government agencies, and provides assistance in assessing, reporting, and correcting DII vulnerabilities. The SCERS program trains a cadre of special agents in state-of-the-art techniques for seizing, protecting, and analyzing computer evidence. The agents are located throughout the U.S. and work closely with primary case agents to ensure that computer searches are complete and thorough. The DCIS will continue to make computer-related crimes an investigative priority and focus its protection efforts towards the DII. *(DoD)*

Audits Reveal Problems in Security Plans for EPA Financial Systems

A number of OIG audits during the fiscal year found significant and pervasive problems regarding the adequacy of security plans for EPA's core financial systems and various regional systems. The audits found that EPA needs to aggressively pursue a quality assurance process to evaluate the adequacy of implemented security plans and the security programs that support them. With a decentralized network that links all EPA computer systems, even one regional location with an inadequate security program can make the entire agency vulnerable. Similarly, weaknesses surrounding key environmental and financial systems could jeopardize the integrity of vital data that decision-makers and the public both use. As a result of OIG's involvement, EPA initiated a centralized validation process for these security plans. *(EPA)*

Collaborative OIG Effort Identifies Potential Fraud in IRS Operations

TIGTA's Strategic Enforcement Division (SED) executes a proactive effort to detect fraud and misuse in Internal Revenue Service computer systems and operations. The program uses advanced computer technology and computer matching to identify criminal violations modeled from criteria identified in prior TIGTA investigations.

SED's operation is an intense, collaborative effort between auditors, special agents, and computer programmers. SED has successfully identified possible fraudulent activities and control weaknesses in IRS operations. The principal component of SED's operation is its national integrity project. SED initiates projects from information developed during a successful investigation. A crime methodology becomes the basis for developing proactive computer database applications that will identify other individuals who may perpetrate the same crime. SED includes these proactive national integrity projects in the Computer Matching Act agreements approved by the Treasury Department's Data Integrity Board and published in the *Federal Register*. *(TIGTA)*

AID Recognized for Progress in Correcting Computer Security Deficiencies

AID OIG issued four audit reports identifying computer security deficiencies that exposed AID to unacceptable risks. Because of these risks, resources and sensitive data located in headquarters and overseas Missions' computer systems might not be adequately protected from loss or destruction. Deficiencies existed because AID had not implemented an effective computer security program as required by the Computer Security Act and OMB Circular A-130.

The OIG found that AID has made and continues to make efforts to correct known deficiencies. For example, during FY 1999, AID officials completed the development of a model information-system security program that provides a framework for identifying and disseminating to other government agencies a complete set of 'best practices' for implementing an effective computer security program. The CIO Council, GSA, and others have recognized the program as an innovative and comprehensive approach that could benefit the entire federal government. Although significant improvements to its information systems security have occurred, AID estimates that computer security vulnerabilities will not be fully corrected until 2003. *(AID)*

VA's Corrective Actions on OIG Findings in Financial Statement Audits Are Incomplete

VA OIG performed audit work during FY 1999 in conjunction with a FY 1998 consolidated financial statement audit. Both audits focused on evaluations of VA's administration of its information security program, access, and monitoring controls, physical security controls, and contingency programs. The OIG found that throughout the VA, corrective actions to improve some automatic data processing (ADP) control issues were incomplete or had not been addressed at the time of the audit. The audit identified significant Department-wide weaknesses concerning information-security policies, oversight, monitoring, and reviews; access to operating systems, applications, and data; contingency programs; and physical access controls. The OIG also found that the VA had taken a number of corrective actions in response to previous audit reports to improve overall general controls at one of three major automation centers. In addition, the VA established the Office of the Assistant Secretary for Information and Technology to better focus attention on ADP security. *(VA)*

II. PART OF THE TEAM: GOVERNMENT PERFORMANCE AND RESULTS ACT

In 1993, the Congress passed and the President signed into law the Government Performance and Results Act (GPRA). Under this law, programs are evaluated on the basis not of outlays or objectives, but of actual results. IGs are an important part of this government-wide initiative. By reviewing their agencies' implementation of GPRA and offering suggestions or recommendations for improvement, IGs are an indispensable part of the team.

IG Community GPRA Oversight Initiatives

The Department of State's OIG founded, serves as the standing chair, and coordinates the programs and activities of the PCIE's Government Performance and Results Act Coordinators Interest Group. The group brings together representatives from across the IG community — as well as OMB, Congress, and other interested organizations — and provides a forum to leverage the community's knowledge, experience, and accomplishments by sharing strategies, best practices, and lessons learned in overseeing agency implementation of GPRA. By providing a common focus for GPRA issues, the group has helped facilitate implementation of GPRA both across government and within the IG community, resulting in broad OIG implementation of the Act's provisions. *(DOS)*

OIG Provides Continuing Input to FDIC Goals and Objectives

FDIC OIG is fully committed to taking an active role in the Corporation's implementation of GPRA. The OIG has developed a GPRA review plan, comprised of three integrated strategies to help ensure that the Corporation satisfies GPRA requirements and has systems in place to reliably measure its progress toward achieving strategic and annual performance goals. These strategies include linking planned audits and evaluations to FDIC's strategic and annual goals and objectives, as well as targeted verification reviews to evaluate the adequacy and reliability of selected information systems and data. The OIG developed a standard work program for these reviews. The third strategy calls for continuing to provide advisory comments as FDIC updates strategic and annual performance plans and reports.

The OIG reviewed a draft of the agency's 2000 performance plan and provided comments regarding Results Act conformance. The OIG also established a GPRA Committee to coordinate all GPRA-related initiatives, and plans to continue PCIE activities related to defining appropriate OIG GPRA roles, responsibilities, and activities. *(FDIC)*

DOE’s GPRA Implementation Is Progressing, But Incomplete

An OIG audit found that DOE was making good progress implementing GPRA in some areas but further action was required. The audit focused on five DOE budget office program requests. The budget requests for the two largest program offices generally demonstrated proper integration between long-term strategic goals and day-to-day activity-level performance data. In addition, these budget requests showed progress in creating measurable and results-oriented performance information. The budget requests for two other offices, however, needed improvement, as they did not clearly integrate activity-level performance data with strategic planning data, and did not include measurable and results-oriented performance standards for which programs and their contractors could be held accountable. Furthermore, none of the program offices had defined processes in place to ensure that all performance data collected from contractors were reliable.

The OIG recommendations focused on strengthening existing policies and guidance to ensure clear integration between DOE strategic documents and information regarding specific activities included in the budget requests. DOE management agreed with the findings and recommendations and believed that the audit would prove useful as the agency continues to implement GPRA. *(DOE)*

Audit Discloses Weaknesses in Processing Concession-contracting Actions

A DOI OIG performance audit report on "Concession Contracting Procedures, National Park Service (NPS)" addressed the NPS’ GPRA accomplishments. The report stated that concession-contracting actions had not been processed in accordance with law or NPS guidance. For example, concession-contracting actions had not been approved as required by authorized officials; contracts were not reissued in a timely manner; and franchise fees had not been periodically "reconsidered." The OIG attributed these deficiencies in part to NPS not having goals in its FY 1999 annual performance plan for processing concession-contracting actions.

The evaluation also discussed performance goal weaknesses related to increasing average returns from concession operations. The performance plan stated that revenues from concessioners would increase from 6.6 percent of gross revenues in 1997 to 7 percent in FY 1998 and 8 percent by September 30, 2002. The goal, however, was based on revenues that came largely from concessioners’ payments to special accounts which, in many cases, were designated to reserve funds that supported concessioners’ facilities. As a result, the payments did not represent a return to NPS. The OIG recommended that NPS include in the annual performance plan specific, quantifiable, and appropriate measures for the concession-contracting program activity, and develop and implement controls to ensure that concession-contracting accomplishments included in the performance plan are reported accurately. *(DOI)*

DOT Performance Plan Rated Tops; OIG to Continue Monitoring GPRA Implementation

Congress recently determined that DOT’s strategic and performance plans were among the best submitted by 24 federal agencies. Although DOT’s strategic and performance plans were highly rated, OIG determined that performance goals needed to be set for: 1) the Federal Aviation Administration’s (FAA) personnel reform initiatives; 2) the Federal Transit Administration’s (FTA) grant-management program; 3) the U.S. Coast

Guard's oversight of private-sector oil-spill response capabilities; and 4) the Federal Railroad Administration's of commuter-rail safety requirements. Additionally, performance goals needed to be completed for 1) FAA's work to halt diversion of airport revenue to non-airport use, and 2) DOT agency efforts to reduce terrorism risks for U.S. passengers at foreign and domestic ports and waterfront facilities.

OIG plans to conduct audits addressing performance measure development and validation of data obtained from accounting systems DOT relies upon to support performance claims. The performance measures will include reducing near-collisions on runways; reducing death and injuries in large-truck crashes; reducing recreational boating fatalities; and reducing rate of air traffic controller operational error. *(DOT)*

AID Overhauls Performance Reporting Guidance in Response to OIG Findings

AID OIG concluded a worldwide audit in March 1999 regarding the quality of reported performance results. The audit, based on a statistical sample of 18 AID operating units, found that these units did not report data in their 1997 results reports that were objectively verifiable, supported, accurate, complete and/or validated. Based on the sample, the audit found problems with 252 of the 302 results reviewed — or 83 percent. Deficiencies in three areas caused the problems. First, operating units often failed to follow policies and procedures when measuring and reporting program performance. Second, AID did not provide sufficient direction and oversight in requiring operating units to follow these policies and procedures. Finally, AID regional and central bureaus needed to more adequately fulfill their responsibilities when assessing operating units' performance and reviewing results reports.

The audit report recommended internal control changes to help ensure that operating units report quality performance data. In response, AID revised its results reporting directives, issued new guidance on what constitutes quality data, and requested that the OIG audit its FY 1999 results reports for possible improvements. *(AID)*

U.S. Secret Service Agrees to Make Improvements in Record Maintenance

The Department of the Treasury OIG reviewed several U.S. Secret Service performance measures and determined that statistics in its Counterfeit Contraband System (CCS) reports were inconsistent. CCS statistics did not agree with those in various FY 1997 accomplishment reports, due to adjustments made by field offices after the end of the fiscal year. Furthermore, the U.S. Secret Service did not maintain records of the adjustments it had made to statistics on counterfeiting. Because adjustments were not accounted for, the OIG was unable to determine the significance of adjustments or the reliability of CCS reports. Following OIG recommendations, U.S. Secret Service officials agreed to maintain adjustment records. In addition, they will update the Service's manual detailing the way in which field offices process counterfeit currency and enter data into the CCS. *(Treasury)*

OIG Expresses Satisfaction with FEMA Efforts to Create Performance-oriented Culture

The OIG is closely monitoring how well FEMA implements GPRA, and is satisfied that it is making a concerted effort to create a performance-oriented culture in the agency. FEMA produced baselines last year for quantitative goals and performance indicators, along with annual performance plans for FYs 1999 and 2000, and is preparing a March 2000 performance report. FEMA has designated GPRA representatives for each of its regions, offices, and directorates. FEMA implemented a quarterly performance reporting system and uses it as one measure of senior managers' performance. The OIG will continue to monitor how effectively FEMA meets the challenge of complying with GPRA requirements. *(FEMA)*

OIG Quantifies Improperly Paid Medicare Fee-for-service Payments at HHS

Although GPRA is in its initial year of implementation, much of HHS OIG's continuing CFO-related work is directly applicable to assessment of HHS-generated, financially related performance data. For example, beginning with OIG's audit of the Health Care Financing Administration's (HCFA) FY 1996 financial statements, and for the first time in the Medicare program, OIG quantified the amount of Medicare fee-for-service payments that were paid improperly during the fiscal year. At the end of FY 1999, OIG estimated that improper fee-for-service payments totaled an estimated $12.6 billion during FY 1998. This represented a 45 percent decline in improper payments since FY 1996.

The OIG attributed the decline in improper payments to several factors: 1) HCFA's efforts under the Medicare Integrity Program; 2) fraud and abuse initiatives; 3) improved provider compliance with Medicare reimbursement rules; 4) HCFA and OIG outreach efforts emphasizing Medicare documentation requirements; and 5) implementation of HCFA's corrective action plan. Although HCFA has made significant progress, recommendations call for HCFA to continue its diligence in reducing past identified problems and to keep abreast of those issues that could negatively affect future error rates. *(HHS)*

OIG Identifies Weaknesses in Controls over GSA Performance Measures

GSA OIG examined the overall design and operation of the internal controls over performance measures reported in GSA's FY 1998 annual report. The OIG concluded that there is no clear understanding of who is responsible for verifying performance data at individual major service organizational levels, or for GSA overall, and that GSA has not adequately defined and documented its system of controls. The OIG stated that this condition could adversely affect GSA's ability to collect, process, record, and summarize performance information.

Management concurred, and GSA's chief financial officer recently established its office as the central data authority responsible for GPRA performance-measurement data used in the annual report, performance plan, other GPRA-required documents, and non-financial budget data. It also asked each Service organization to designate an office responsible for ensuring that transactions and other data that support reported performance measures are properly recorded, processed, and summarized. Steps would then be taken to improve and document procedures and internal controls. *(GSA)*

NASA Agrees to Implement OIG Recommendations on Performance Goals

NASA has made substantial progress in implementing GPRA, including preparing and updating its strategic plan and issuing performance plans for FYs 1999 and 2000. The OIG's review of NASA implementation actions, however, identified two areas involving the FY 1999 Performance Plan that management needs to improve. First, senior management oversight of overall progress was inadequate for established FY 1999 performance targets. Second, management had not established appropriate procedures to ensure the data it would use (both to measure interim progress and to describe final results in the annual performance report) were accurate and reliable. Management agreed with recommended actions to ensure that senior managers effectively evaluate progress on the established performance goals and that performance data are accurate and reliable. *(NASA)*

OIG Actively Promotes Improvement of EPA Operations

Consistent with the IG Act, the EPA OIG has actively promoted improvement of EPA operations by overseeing effective implementation of GPRA provisions and assisting agency managers to institutionalize GPRA principles into day-to-day operations. OIG is assisting EPA in evaluating how well it accomplishes its goals, ensures the adequacy of its accountability systems, and develops meaningful performance measures. Future OIG audits will evaluate the accuracy, adequacy, and reliability of data needed to measure performance and environmental results of EPA operations, and its grantees and contractors, in managing the nation's water quality and cleaning up the nation's hazardous-waste sites. The OIG is also reviewing EPA's cost accounting procedures, processes, and systems to determine the costs of obtaining each goal. In addition, the OIG is using new tools and approaches to help EPA integrate GPRA implementation into its products and services.

The OIG has developed and is using the following new tools and approaches for integrating reviews of and assistance for EPA's GPRA implementation into its products and services: 1) GPRA Review Guide for assessing implementation of GPRA requirements by EPA; 2) audit planning/reporting process linking products and services to Agency strategic and annual performance goals, environmental outcomes, measures, data, and management challenges; 3) survey of agency data systems and sources for selected goals and vital measures; and 4) customer/market approach to planning, performance, and assessment of products and services. *(EPA)*

OPM Incorporates Many OIG Suggestions into Its Performance Plan

The Office of Personnel Management's compliance with GPRA is one of the OIG's principal ongoing review areas. During FY 1999, the OIG participated as an advisor as OPM developed its FY 2000 annual performance plan by providing review, commentary, and recommendations for improvement. While OPM incorporated many OIG suggestions into the final documents, the OIG identified two remaining major areas of weaknesses: 1) the lack of cost-based performance measures in some areas to show how efficiently OPM performs certain operations and activities; and 2) limited confidence that agency performance information will be credible.

The outcome of OPM's first efforts to implement GPRA was seen in its first annual program performance report, which it submitted to the President and Congress in March 2000. This submission culminated OPM's first strategic planning cycle, providing information on actual performance and progress toward the goals and objectives iterated in the strategic and annual performance plans. OIG auditors and evaluators have begun to independently perform reviews intended to verify and validate the performance data that were reflected in this report. *(OPM)*

OIG Takes Active Role in Postal Service’s Compliance with GPRA

The U.S. Postal Service's *CustomerPerfect!* performance measurement system complements GPRA, supporting the law's mandate to establish a set of measurable goals while upholding the USPS mission and defining strategies to achieve these goals. The OIG has taken an active role in USPS's compliance with GPRA, assessing the agency’s implementation of GAO's reported observations about its draft strategic plan and preliminary annual performance plan. In general, USPS included additional information identified by GAO in its reports. However, the OIG suggested that USPS could enhance its future plans by including more detailed discussions of specific areas. *(USPS)*

OIG Assesses Integrity and Accuracy of VA Data

In FY 1998, VA OIG initiated a multi-stage audit to examine the integrity of data used in GPRA reports. Following upon this effort, during FY 1999, the OIG assessed: 1) data integrity for the Veterans Benefit Administration’s (VBA) processing of veterans claims; 2) the accuracy of National Cemetery Administration (NCA) data used to measure the percentage of veterans with a VA burial option; and 3) the accuracy of data used in Veterans Health Administration (VHA) to count the number of unique patients.

The OIG found that VBA needs to improve the accuracy of data input on claims-processing timeliness. NCA personnel generally made sound decisions and accurate calculations when preparing their estimates, though NCA needs to retain some data longer. VHA’s unique-patients data overstated actual usage by six percent because inaccurate Social Security numbers were input, and because appointment cancellations and no-shows were sometimes counted as being treated. The OIG recommended corrective actions in all cases. *(VA)*

SBA Section 504 Job Creation Data May Be Unreliable

SBA’s Section 504 loan program provides long-term, fixed-rate financing to small businesses for the purchase of land, buildings, machinery, or other fixed assets. The program is delivered through nonprofit Certified Development Companies (CDCs) established to promote local economic development. By regulation, CDC loan portfolios must create or retain one job for every $35,000 in debenture proceeds that SBA provides. The Section 504 program represented approximately 15 percent of SBA's business loan funding in FY 1999.

An OIG inspection found that CDC job creation data currently being used in SBA's GPRA plans has not been verified, and has serious methodological flaws that call into question its reliability. While SBA collects CDC job creation data, it is inconsistent and, for portfolio management purposes, adds together estimated and actual jobs created. In addition, the reported data is based on an unverified estimate of how many jobs Section 504 funding has created or retained at some unidentified point in the past. *(SBA)*

OIG Performs GPRA Reviews for Three USDA Agencies

USDA OIG examined three USDA agencies' activities pursuant to GPRA. OIG examined a segment of the Food and Nutrition Service's strategic goal dealing with the Child and Adult Care Food program. Specifically, OIG reviewed the segment calling for "better targeted and higher quality program reviews of sponsors and providers by state agencies" and the associated indicator "number of reviews conducted." OIG determined that while the strategic goal was valid, the performance measure was vague, and did not include any quantitative measurement data.

OIG also examined a segment of the Forest Service's strategic goal to "ensure organizational effectiveness." Specifically, OIG reviewed the management initiative calling for "a sound financial system which supports resource decisions with timely, accurate information and financial expertise." OIG determined the initiative to be valid but found mixed results regarding the primary performance measures. Finally, OIG examined a segment of the Risk Management Agency's strategic plan objective to "improve program integrity and protect taxpayers' funds," specifically, the strategic goal intended to "reduce program vulnerabilities." OIG concluded that the goal is valid but questioned some of the data reported. *(USDA)*

OIG Recommends Improvements on NLRB Performance Plan

NLRB OIG reviewed NLRB's FY 2000 performance plan and informed management that it needed improvement in three areas. The OIG suggested that management streamline the report by tying goals to program areas. Next, the OIG recommended that NLRB reconsider performance measures that were not objective, measurable, and verifiable. Third, the plan should provide additional information about how NLRB intends to verify and validate performance data. *(NLRB)*

OIG Monitors Progress and Suggests Improvements to NSF's GPRA System

NSF OIG participated in internal agency working groups tasked to revise NSF's strategic plan, develop performance plans for future years, and develop its first annual performance report. Where appropriate, the OIG offered NSF's management suggestions, primarily related to data and measurement issues, that may affect the success of its GPRA system. The OIG also participated in a working group that is monitoring the activities of an outside contractor assessing the quality of NSF data.

The OIG has also incorporated consideration of performance data systems in its ongoing efficiency reviews. For example, the OIG tested the validity of some data provided by NSF-supported researchers about a statistically valid sample of information that NSF management could consider during its assessment of program performance, and found the information was generally accurate. *(NSF)*

OIG Review Finds Problems with Half of SEC's Performance Measures

SEC OIG reviewed the support for a sample of 16 FY 1997 performance measures in the Commission's 1999 GPRA performance plan. The review found that half of those measures (eight) did not materially agree with the supporting records.

Like other federal agencies, SEC apparently encountered difficulties in the definition, data collection, and reporting phases of performance measurement. Besides recommendations to improve the supporting records, the OIG recommended additional GPRA training and guidance, and improved controls in GPRA-related tracking systems. *(SEC)*

OIG Reviews ITC's Ability to Report on Performance Measurement Goals

ITC OIG conducted a review to verify and validate selected data sources and information collection systems that supported ITC's FY 1999 annual performance plan. OIG found considerable improvement over the form and content of the performance measurement goals in the 1997 strategic plan. The various office directors with responsibility for performance goals were collecting data or making plans for virtually all performance indicators. In a few instances, OIG found that the data sources and information collection systems did not identify the customers who used them, establish critical dates needed to evaluate measurement of the performance goal, and in a few instances, indicate where performance goals and indicators could be clarified.

The OIG suggested that the Director of Operations determine whether strategic goals for customers' use apply to the individual types of customers identified, or non-ITC use in general, and ensure that data-collection systems include all necessary dates to measure timeliness. The Director of Operations implemented changes that included modifying some customer-use measures, and expanded some data collection systems. In addition, the next version of the strategic plan will include clarified language for some goals, and other goals may be revised or eliminated. *(ITC)*

ED Benefits from OIG Technical Assistance in Developing Data-quality Standards

In an earlier audit report assessing ED's implementation of GPRA, the OIG recommended that ED establish controls over the analysis and reporting of data, establish standards for reporting performance information and establish a formal system for tracking indicators. During FY 1999, the OIG provided technical assistance to the Department as it developed draft data-quality standards and training on those standards. ED used these standards in verifying and validating data for the its FY 1999 performance report. The OIG reviewed drafts of ED's FY 1999 performance report and FY 2001 annual plan and provided comments, many of which the Department accepted. *(ED)*

OIG Finds FLRA Successful in Implementing GPRA at All Levels

FLRA OIG found that FLRA had made a noteworthy commitment during FY 1999 to comply with GPRA, and to meet congressional expectations for mission-oriented strategic planning and performance measurement. The very visible support and involvement of FLRA executive leadership was instrumental in making this agency-wide initiative successful, involving participation at all levels. The OIG found that in addition to the agency's strategic plan, each FLRA organizational component had action plans to support the agency's mission-related goals. In addition, each FLRA employee had a work plan, updated yearly, supporting his or her organization's action plan. *(FLRA)*

The OIG also found that performance measurements were both qualitative and quantitative. The single vulnerability that surfaced during this review was the inconsistency and the questionable credibility of data in some parts of the organization. Also noted was the fact that even though crosscutting activities and weaknesses that emerged through external and internal oversight activities were discussed during the strategic planning process, their impact was not discussed in the final documentation. FLRA has advised OIG that management will focus on correcting data inconsistencies during this coming year before it provides its first "Baseline Performance Measurement" report to Congress. *(FLRA)*

Six OIG Audits Assess TVA Indicators' Adequacy and Reliability

TVA OIG performed six audits during FY 1999 pertaining to indicators TVA provided to Congress as part of its strategic plan to comply with the Government Performance and Results Act. The objective in each audit was to assess the adequacy and reliability of the information used to calculate the indicator. The OIG determined in five of these audits that the information used to calculate the indicators was adequate and reliable.

The review of the remaining indicator, TVA's Dam Safety Performance Indicator, determined that TVA could improve the reliability of its data sources and information systems and thus its compliance with federal guidelines. In an effort to correct deficiencies the audit identified, TVA management implemented a new dam safety organizational structure and established three teams to map and correct key program components. *(TVA)*

FCC Concurs with OIG Recommendations; Will Completely Revise Strategic Plan

FCC OIG reviewed FCC's GPRA and performance goal implementation for FY 2000. The OIG determined that, while making significant strides in meeting GPRA requirements, the Commission's performance plans contained primarily output-based rather than outcome-oriented annual performance goals. The report contained recommendations that the Commission take necessary actions to address this condition by developing outcome-based performance goals. Management concurred with OIG recommendations and began a complete revision of the Commission's FY 2001 strategic plan. *(FCC)*

III. INTEGRITY, ACCOUNTABILITY AND RESULTS

The work of IGs can bring about not only financial, programmatic, and management improvements, but also improvements that change people's lives. Last year, Inspector General findings and recommendations led agencies to agree to or implement changes that will make a positive difference in the lives of those who are served by their programs.

OIG Assessments of GSA Security Efforts after Oklahoma City Bombing Continue to Identify Needed Improvements

In the aftermath of the 1995 Oklahoma City bombing, the sensitivity of GSA's security mission has heightened greatly. GSA has taken positive steps toward enhancing the level of physical security nationwide, and the OIG has performed reviews to assess the agency's progress.

In FY 1996, the OIG determined that GSA had not materially changed its construction guidelines and criteria describing how specific construction techniques and the employment of security measures can deter acts of terrorism and lessen the effects of external blasts. A FY 1999 follow-up review disclosed that GSA had worked aggressively with other federal agencies to develop a comprehensive set of physical security standards for new and major renovation construction projects, and is applying enhanced security standards where possible for new construction projects.

Focusing on upgrading security at federal facilities during FYs 1998 and 1999, the OIG reported that GSA was not accurately reporting the status of security-enhancement equipment installation, had misused enhancement funding, and had not planned for the use of about $2 million of equipment found in storage. Subsequent reviews conducted at specific facilities to assess the status of security countermeasures implemented has disclosed that, while GSA has made progress in addressing building security concerns, it still needs to complete steps designed to provide better security within government facilities. The OIG is now evaluating GSA's Contract Security Guard program, and will continue to assess GSA’s progress toward addressing security issues. *(GSA)*

OIG Estimates $229 Million in Unallowable Payments to Community Mental Health Centers

With the Heath Care Financing Administration (HCFA), HHS OIG reviewed Medicare payments for partial hospitalization services to community mental health centers (CMHCs) in five states. The OIG estimated for FY 1997 that Medicare paid these CMHCs $229 million for unallowable and highly questionable services; this represented 91 percent of the total $252 million paid to all CMHCs in these five states for partial hospitalization services.

In a program designed to pay for intensive outpatient psychiatric services for acutely ill individuals who would otherwise require inpatient services, OIG determined that Medicare was paying for services to beneficiaries who had no history of mental illness, or who suffered from mental conditions that would preclude their benefiting from the program. Further, Medicare was paying for therapy sessions that involved only recreational and diversionary activities. The lack of state oversight and the use of a self-attestation process permitted unscrupulous providers to participate in the Medicare program.

In view of the severity of the problems disclosed, OIG recommended that HCFA evaluate the propriety of allowing CMHCs to provide the partial hospitalization benefit and, if appropriate, recommend a legislative change to repeal Medicare coverage for this benefit in the CMHC setting. Also, OIG reiterated recommendations made in an earlier review of 14 CMHCs in Florida and Pennsylvania to address these concerns. The HCFA developed a 10-point initiative including both immediate and long-term actions, such as terminating egregious CMHCs, conducting intensified medical reviews, collecting overpayments, and undertaking various legislative actions. *(HHS)*

Review Recommends DOJ Take Actions to Curb Inmate Abuse of Telephone Privileges

A DOJ OIG review disclosed that federal inmates were using prison telephones to commit serious crimes while incarcerated—including instances of arranging for murders, drug trafficking, and fraud. Telephone privileges for Bureau of Prisons (BOP) inmates have increased dramatically since the 1970s, when inmates were permitted one telephone call every three months, which a staff member placed. Now, most inmates are allowed to make as many calls as they can afford, or as many collect calls as outsiders will accept.

The OIG found that, although BOP has been aware of inmates’ abuse of prison telephones for some time, it has taken insufficient steps to address the problem. For example, while all inmate calls are recorded, BOP staff listened to less than 4 percent.

The review also found that inmates who had been convicted of committing crimes using prison telephones still enjoyed full telephone privileges. The OIG recommended that BOP curb prison telephone abuse by monitoring more calls, increasing and exercising more consistency in the discipline of telephone abusers, restricting telephone privileges for inmates with a history of abuse, and emphasizing to officers the responsibility to detect and deter crime. *(DOJ)*

OIG Motor Carrier Safety Work Spurs Congress to Create New Truck Safety Agency at DOT

Motor vehicle crashes claim more lives in the U.S. than any other mode of transportation – at least 40,000 deaths per year, some 5,300 involving large trucks. Last year the Department of Transportation OIG's auditors and investigators brought significant expertise to improve trucking safety as they produced definitive reports and substantial congressional testimony. They also investigated criminal cases, leading to 34 convictions and $3.7 million in fines and restitution for offenses ranging from falsification of truck drivers' logs to bribe acceptance by officials who administer truck drivers' licensing tests. OIG's auditors found that because DOT's main oversight agency has shifted emphasis away from enforcement, few company-wide inspections (known as "compliance reviews") are conducted, and when such reviews find violations that lead to fines, those fines are often reduced to levels that fail to deter future violations. Finally, responding to OIG recommendations, Congress created the new federal Motor Carrier Safety Administration within DOT. *(DOT)*

FDIC OIG Is a Catalyst for Proposed Legislative Change

Over the past several years, the nation's banking industry has experienced unprecedented consolidation resulting in extremely large and complex financial conglomerates. Of the $4.5 trillion in assets controlled by the 39 largest institutions, FDIC is the primary federal regulator for only two of these institutions, amounting to $77 billion of the assets. Since the FDIC does not maintain a presence in the other 37 institutions, it depends heavily on other federal regulators to provide information to monitor these banks' insurance risks.

The OIG reviewed FDIC's efforts to monitor risk at the insured institutions where it is not the primary federal regulator. The OIG focused on the backup examination process for insured thrifts, national and state member banks, and FDIC's efforts to monitor risks associated with the largest and most complex financial institutions. The OIG issued a memorandum to the FDIC Chairman with suggestions to strengthen the cooperation between FDIC and other federal banking regulators and to improve the effectiveness with which FDIC carries out its responsibility to monitor insurance risk.

The OIG shared its concerns with the House Committee on Banking and Financial Services. The Committee Chair, Rep. James A. Leach, introduced a bill that would strengthen the FDIC's independence by: 1) granting back-up examination authority to the FDIC Chairman, and 2) requiring banking agencies to establish information-sharing procedures to ensure that the FDIC has sufficient information to assess risk to insurance funds. *(FDIC)*

OIG Investigations Lead to Convictions and Changes in Education's Student Aid Programs

ED OIG has devoted significant resources to identifying and prosecuting fraud against ED's student financial assistance programs and to identifying, and recommending corrective actions to address the systemic weaknesses that allow them to occur. For example, during FY 1999, one investigative initiative focused on consultants who assist students and parents in reporting false income and other financial data to obtain student financial aid to which they are not entitled. In one case, a Michigan consultant was sentenced to 40 months imprisonment and was ordered to pay $1.7 million in restitution; in another, a New York consultant admitted guilt and was sentenced to 12 months imprisonment and was ordered to pay a $15,000 fine. Both cases involved the preparation of false applications for student aid, as well as fraudulent tax returns and other supporting documentation which ED and colleges use in awarding financial aid.

Another OIG concern has been the inappropriate discharge of student loans based on disability or death. The Higher Education Act Amendments of 1998 provide for the discharge of a student loan when the borrower becomes totally and permanently disabled or dies. As a result of a request by the Department, OIG conducted a review that disclosed persons who had received loan discharges based on death or disability but were earning wages subsequent to the discharge. OIG continues to pursue this matter, and is engaged in a project to identify those instances that were caused by error or were a result of fraudulent applications for disability and death discharges. OIG recommended that the Department take several steps to enhance the current discharge determination procedures, including revising the disability form to include, at a minimum, the doctor's professional license number and office telephone number, and requiring certified copies of death certificates. In response, the Department modified its disability form to incorporate OIG's recommendations. In addition, the Department now requires that a death discharge be based only on an original or certified copy of the death certificate. *(ED)*

OIG Finds DOE Waste Incinerator Operates Below Capacity and Generates Excessive Costs

The Toxic Substances Control Act (TSCA) incinerator treats radioactively contaminated polychlorinated biphenyl (PCB) waste, and is located at the East Tennessee Technology Park in Oak Ridge, Tennessee. An OIG review found that the DOE contractor did not operate the incinerator at the annual burn rate permitted by the State of Tennessee, or at the "attainable" capacity that represents the more realistic burn rate determined by the operating contractor. Had the DOE more aggressively incinerated the waste, the 7.7 million pounds incinerated could have been incinerated in one year rather than three, at a savings of about $24 million. Furthermore, the waste could be treated more economically at commercial facilities, once these treatment options become available in June 2000.

The OIG concluded that all of Oak Ridge Reservation's existing incinerable-waste inventory could be treated by June 2000, at which time the incinerator could close, 39 months earlier than planned, and reduce operating costs by $39 million. The OIG recommended that DOE: 1) require the contractor to characterize the inventory of incinerable waste as soon as possible to facilitate preparation of a burn plan that will allow the TSCA incinerator to operate more efficiently, and 2) close the TSCA incinerator as soon as other treatment options are in place. DOE management concurred with the finding and recommendations and initiated corrective actions. *(DOE)*

Inefficient Use of DOI Grant Funds Leaves Students Without Classrooms

After unsafe conditions forced the closure of federally owned portable classrooms at the Lac Courte Oreille Ojibwe School, the Bureau of Indian Affairs (BIA) granted $2,550,000 for the design and construction of replacement facilities, including $180,000 for leasing temporary space. DOI OIG reviewed this use of funds and found that school officials 1) attempted to replace 17,359 square feet of portable classrooms with a 41,358 square-foot building without having the necessary financial resources to complete the larger structure; 2) used operation and maintenance funds intended for leased space to construct another 8,500 square-foot school building; 3) invested grant funds in a retail operation; and 4) did not follow applicable procurement requirements when awarding a contract for construction of the 41,358-square-foot building. In addition, the OIG questioned the allowability of $450,922 in grant funds that were spent for activities outside the scope of the grant agreements or otherwise did not comply with federal cost principles. As a result of these deficiencies, a 41,358 square-foot building that students cannot use is incomplete; grant funds were at risk of loss, because they were invested in an operation that was not fully guaranteed or insured; there was a lack of assurance that construction costs were fair and reasonable; and the questionable grant expenditures of $450,922 may have to be returned to BIA. *(DOI)*

OIG Inquiry Reveals Deficiencies in NRC Investigations

NRC OIG, in response to a request from three members of the Connecticut congressional delegation, reviewed the process and specific conclusions reached at the close of several investigations conducted by the NRC Office of Investigations. These investigations dealt with complaints of harassment and intimidation by several former employees laid off from work at a nuclear power plant in Connecticut.

The OIG inquiry revealed deficiencies in the documentation process that NRC staff followed in reaching a conclusion regarding enforcement action in one case. Additionally, the OIG found that portions of staff briefings given to NRC were not clear with regard to the staff’s intended actions. Finally, the OIG found that the staff had insufficient information upon which to base a conclusion contained in their written correspondence with some of the individuals who had made allegations. *(NRC)*

OIG Audit Helps Texas Colonia Residents Obtain Water and Sewer Connections

In response to an EPA OIG audit, the Texas Water Development Board adopted a new policy allowing federal funds to help residents of colonias obtain water and sewer connections. Colonias are small communities along the U.S.-Mexican border which are often impoverished, with substandard housing and poor living conditions. The audit revealed that many colonia residents could not afford to connect their homes to wastewater treatment facilities, and there were no provisions under the prevailing assistance program to fund connection costs. OIG recommended that EPA help develop affordable financial strategies for residents to receive services. In one region alone, OIG estimates that implementation of the new policy will allow $12 million in federal money to be spent on household connections to water and wastewater lines. About 10,000 households containing approximately 40,000 to 50,000 people could benefit from this policy. *(EPA)*

Criminal Matters Involving the Misconduct of VA Employees

In FY 1999, the OIG resolved 217 cases of VA employees involved in criminal misconduct, which resulted in 104 indictments, 74 arrests, 64 convictions, 14 terminations from position, and more than $6.6 million in fines and restitution. In addition, VA officials took 120 administrative actions. Two examples of these misconduct cases follow.

- ➢ A former VA supervisor was sentenced to 33 months in prison and ordered to pay VA $615,472 in restitution and forfeit over $300,000 in property. The OIG disclosed the supervisor created computerized benefit records that fraudulently reflected that her fiancé was entitled to receive VA disability payments.

- ➢ A former VA ratings specialist was sentenced to 33 months' imprisonment, 3 years' supervised release, and ordered to pay VA $588,872 in restitution. The OIG revealed he had created a record for a fictitious veteran for service connected-disabilities. In 12 years he received over $588,000. *(VA)*

Audits of Federal Employees Health Benefits Program Focus on Integrity Issues at OPM

During FY 1999, OPM OIG issued final reports on audits of 53 carriers participating in the Federal Employees Health Benefits Program (FEHBP), the largest employer-sponsored health insurance program in the nation. The FEHPB makes annual outlays of approximately $17 billion and furnishes health care coverage to over 9 million persons. The audit reports collectively contained questioned costs of approximately $95.1 million, a sum equivalent to OIG's long-term annual averages for both reports issued and costs questioned.

Because FEHBP provides benefits through private sector insurance carriers, it faces the same integrity issues that challenge the American health-care system at large. These issues are the focus of a major and continuing OIG effort that has three principal objectives: 1) determining compliance of program participants with the laws, regulations, and contracts through which FEHBP is operated; 2) recovering funds improperly incurred or paid; and 3) protecting the health and safety of federal employees, annuitants, and eligible family members who obtain FEHBP coverage. *(OPM)*

OIG Recommendations Will Result in $48 Million Transfer to RRB Trust Funds

In 1951, amendments to the Railroad Retirement Act introduced the concept of financial interchange between RRB and SSA. The interchange places Social Security trust funds in the same financial position in which they would have been had the Social Security Act and the Federal Insurance Contributions Act covered railroad employment.

The financial interchange is a major source of funding for benefits payable under the Railroad Retirement Act. Since the amendments became law, the two agencies formally agree each year on estimates of additional benefits and administrative expenses that would have been paid from the Social Security trust funds and additional payroll and income taxes that would have been collected, including interest. The most recent OIG audit concerned the inclusion of unrecovered overpayments in the financial interchange calculations. While RRB and SSA have had discussions about this matter in the past, without reaching an agreement, RRB actuaries have agreed to present OIG's most recent report to SSA officials to seek concurrence. When implemented, auditors estimated the financial impact of a one-time transfer will be $48 million (including $18 million in interest) to the RRB trust funds related to 1985-1997 and $2 million for each year thereafter. *(RRB)*

DOS OIG Focuses on Embassy Physical Security

In the year since the tragic bombing of the U.S. Embassies in Nairobi and Dar es Salaam, DOS OIG substantially expanded its oversight of embassy security and initiated reviews of DOS's management of the FY 1999 $1.5 billion Emergency Security Appropriation (ESA). The OIG mobilized a multidisciplinary inspection and audit effort to identify physical security vulnerabilities, and to evaluate execution of emergency planning, and management of ESA initiatives. OIG inspected 40 embassies, most of which lacked the setback needed to give some protection from large vehicle bombs.

The Department initially questioned the OIG's September 1998 recommendation for a new imminent-danger alarm system providing warning for embassy employees to "duck and cover" in the event of a vehicle-bomb attack threat. The Department subsequently accepted the recommendation. OIG's embassy inspections contributed to more effective and rapid implementation of the alarms while also stressing the need for timely, frequent "duck and cover" drills, especially at missions lacking adequate setback. The Department also implemented dozens of other OIG recommendations to minimize security vulnerabilities and improve construction of Nairobi and Dar es Salaam's interim office facilities. The OIG found ESA-funded procurement programs and security recruitment and training initiatives to be generally well managed and coordinated, but recommended measures to improve the efficiency and accuracy of accounting for ESA funding.

The OIG also extended its security oversight to the Broadcasting Board of Governors' (BBG) engineering components and broadcasting networks, which has resulted in recommendations for substantial improvements in security preparedness at overseas as well as domestic facilities. These recommendations have been endorsed by the BBG and several of the corrective actions are underway. *(DOS)*

OIG Projects $4.3 Million in Disallowed Costs if USIA Implements Recommendations

DOS OIG reviewed a grantee's proposed indirect-cost pools and the associated indirect rates for FY 1999. The grantee was a nonprofit corporation that developed, administered and provided technical assistance to international education and exchange programs. OIG analyzed the allowability and allocability of accounts comprising the grantee's indirect proposals, including specific indirect costs such as facility and administrative expenses.

The review questioned $1,054,098 of the costs proposed in the indirect-cost-rate calculations because of the organization's proposed accounting treatment of transactions involving the sale of a building and subsequent leaseback of that same building. The grantee's proposed accounting methodologies did not comply with OMB Circular A-122, which limits allowable rental costs on sale and leaseback arrangements to the amount that would have been allowed had the grantee continued to own the building. OIG projected a total of $4.3 million in disallowed rental costs over the life of the lease. *(DOS)*

OIG Inspection Identifies "Paperless Environment" Issues at SBA

An SBA OIG inspection identified security, legal, and organizational challenges that public- and private-sector managers need to address before converting existing paper-based procedures to electronic processes. This study was a significant proactive effort to prevent problems that can disrupt programs when resource-starved managers attempt such conversions with insufficient preparation.

In non-technical language, the inspection report and a companion checklist guide describe how informed program managers can significantly: 1) reduce security risks from inadvertent leaks of sensitive information to deliberate attempts to exploit system vulnerabilities and commit crimes; 2) minimize legal risks, from liability for safeguarding proprietary information to evidentiary problems in court; and 3) reduce organizational problems, such as the threat that employees may perceive when new technology is introduced to assume some of their functions. The report has been well received by both private- and public-sector organizations as a useful roadmap for converting their processes. *(SBA)*

Audit Identifies Nearly $1 Billion in Savings in USPS Corporate Call Management Program

The Corporate Call Management program is a new USPS program that utilizes a network of service centers that offer USPS customers easy access to services and products anytime, anywhere, via a 1-800 toll-free number. The OIG audited the program, which was designed to enhance customer service, and found that technology advances and other changes would permit USPS to reduce the original scope of the $3.4 billion program. OIG was advised that the Postal Service Board of Governors never approved the decision analysis report, and that the project was to be phased in over time, and was approved on that basis.

At the OIG's suggestion, officials revised the model and recalculated operating and investment costs. As a result of OIG's audit and USPS management slowing the implementation process, USPS recognized a potential cost avoidance of $962 million through FY 2007. Management agreed with a recommendation to notify the Board of Governors of the cost reduction, and agreed to notify them, via quarterly reports, of future cost reductions as they are realized. (*USPS)*

OIG Identifies Management Control Weaknesses in Bureau of Alcohol, Tobacco and Firearms

A Department of the Treasury OIG audit of the Bureau of Alcohol, Tobacco and Firearms' (ATF) controls over tax-free exports of distilled spirits found management control weaknesses in several areas. The weaknesses related to: 1) reviewing the adequacy of export evidence that supported claimed exports (the OIG estimated that ATF could have assessed at least $66.6 million in taxes on shipments); 2) updating ATF export-tracking logs to ensure that distilled-spirit plants submitted export evidence (as of August 1998, ATF had not closed claimed export shipments with associated taxes of $560 million for 1996 and 1997); and 3) conducting more third-party verifications of exported shipments. Factors contributing to these control weaknesses included a paper-laden manual process and review system; unclear regulatory and internal guidance over specific documentation requirements; lack of enforcement action and sanctions; and resource constraints.

The OIG made seven recommendations addressing the reported control weaknesses. These recommendations included assessing $66.6 million in excise taxes, plus interest, clarifying existing guidance, and increasing the use of third-party verification. ATF concurred with the findings and recommendations in OIG's draft report and has initiated corrective actions. Additionally, ATF has reconciled and cleared $536 of $560 million in open shipments and is continuing to resolve the remaining $24 million open shipments. *(Treasury)*

Commerce OIG Helping Increase Accuracy and Control Cost of 2000 Decennial Census

The decennial census is an enormous and complex undertaking. The accuracy of decennial data is critical because it is the basis for apportioning seats in the House of Representatives, and is used to support a host of other significant activities. Given the complexity and importance of the 2000 Decennial Census, DOC OIG made oversight of decennial planning one of its top priorities during FY 1999. The OIG issued five major reports on a wide range of decennial issues, making recommendations addressing problems with Bureau of the Census processes and operations, some of which, if not corrected, could have serious implications for the decennial. In all cases, the bureau worked hard to address OIG concerns, taking many immediate corrective actions designed to meet the dual goals of increasing the accuracy and controlling the cost of the Census. *(DOC)*

OIG Questions Results of SSA Survey That Reached Fewer Disabled Customers

SSA OIG conducted a review to determine the reliability of the data used to measure SSA customer satisfaction. The OIG found that while the customer satisfaction survey accurately measured customer satisfaction for the population that it reached, the survey did not reach all types of customers. Additionally, the proportion of disabled customers in the survey sample was less that in previous years. The OIG believed that, since disabled customers have historically provided lower ratings of satisfaction, the lower proportion of disabled customers in the survey may have led to the increased level of overall customer satisfaction when compared to prior years. *(SSA)*

Auditors Report on FEMA's FY 1998 Financial Statements

FY 1998 was the first year FEMA prepared agency-wide financial statements, including the first complete set of statements for the Disaster Relief Fund. OIG auditors gave the statements an unqualified opinion, meaning they were fairly presented and free of material misstatements. In addition, OIG noted improvement in FEMA's ability to comply with laws and regulations, most notably in meeting the statutory deadline of March 1, 1999, for the FY 1998 agency-wide financial statements. However, OIG noted material weaknesses that prevented FEMA's full compliance with the Federal Financial Management Improvement Act (FFMIA) of 1996. The OIG will continue to work with FEMA's Office of Financial Management to improve internal controls in order to meet the FFMIA objectives. *(FEMA)*

Follow-up Review at HUD Finds Limited Improvement

HUD OIG performed a follow-up review to a 1997 audit of HUD's procurement activities that had found significant weaknesses in HUD's procurement systems. The follow-up review assessed effects of recent procurement-process reform initiatives intended to increase safeguards against fraud, waste, and abuse.

Since the initial audit, HUD hired a chief procurement officer (CPO), established a Contracts Management Review Board, and assigned trained, full-time technical representatives to oversee contracts. Further, the recently deployed HUD Procurement System (HPS) now links procurement with core accounting systems. The HPS provides for tracking contract status from planning through post-award contract administration. While the CPO's commitment to make HUD a model procurement agency is encouraging, the OIG is not convinced that HUD's overall contracting attitudes and practices have changed significantly from two years ago. Indeed, many planned improvements appeared more substantial on paper than in reality. *(HUD)*

Joint OIG Review of Federal Financial Institutions Examination Council's Training Program

The IGs of the Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, Department of the Treasury, and National Credit Union Administration completed a joint review in March 1999 of the Federal Financial Institutions Examination Council's training program. In establishing the Council in 1979, the Congress directed it to conduct schools for examiners of the five member agencies as well as state and foreign financial institution supervisory agency employees. Member agencies use the Council's training program as a supplement to their own examiner education programs and spend about $1.5 million annually for these courses.

Although the Council had met its legislative mandate, the joint review team recommended improvements to the strategic planning, information sharing, budgeting, and funding approaches of the Council's training program. The Council was receptive to the recommendations and requested additional guidance from the OIGs on a consultative basis as the Council implements the recommendations. As the lead agency, FDIC OIG will periodically monitor the status of the recommended actions and report on progress in its semiannual report to the Congress. *(FDIC)*

OIG Evaluation Helps NASA Improve Management of Export-controlled Technologies

NASA OIG evaluated NASA's control of export-controlled technologies. The OIG determined that NASA has not identified all export-related technologies related to its major programs, and does not maintain a catalog of classifications for transfers of export-controlled technologies. The audit also showed that NASA's oversight of training for personnel in the Export Control program needs improvement. Specifically, management had not adequately performed annual audits of each Center's export control system, and NASA personnel lack training in controlling and documenting export-controlled technologies. Improvements are necessary to ensure that controls over export-controlled technologies are sufficient to preclude unauthorized or unlicensed transfers.

The OIG made six recommendations to ensure that a cataloging process for export-controlled technologies is developed, that only qualified personnel perform the agency's export control audits, and that employees involved directly or indirectly with technology are trained in properly classifying and protecting export-controlled technologies. NASA has now established classifications for export-controlled technologies and has initiated a more rigorous training program. Management is visiting each NASA center to discuss export control and to conduct training, and is preparing a policy directive, procedures, and guidelines on export control. *(NASA)*

Operation "Kiddie Care" Finds Structural Flaws, Unscrupulous Sponsors in USDA Program

Operation “Kiddie Care,” USDA OIG’s initiative to identify, remove, and prosecute unscrupulous Child and Adult Care Food program (CACFP)-sponsoring organizations, continued to be successful during FY 1999. The focus of the operation is now on improving program delivery and oversight. As an outgrowth of Operation “Kiddie Care,” OIG is emphasizing the need for regulatory and legislative changes in CACFP.

In its national audit report, OIG made 23 recommendations to eliminate the structural program flaws, strengthen internal controls, and clarify program requirements in CACFP. OIG also recommended that alternative methods of delivery be studied. Twenty sponsoring organizations receiving approximately $42.3 million annually in food and administrative funds have been terminated from CACFP. Thirty-four individuals have pled guilty or were convicted, and 29 individuals were sentenced for their illegal activities. Among those recently convicted after investigation by OIG were the president and assistant of a day-care operation in Michigan. They were found guilty of fraud, embezzlement, conspiracy, and money laundering related to defrauding CACFP of an estimated $17 million between 1989 and 1993. The jury also awarded forfeiture of more than $1.1 million in cash and three properties. *(USDA)*

OIG Finds Treasury Overcharged DOL’s Unemployment Trust Fund $48 Million

DOL OIG audited administrative charges to the Unemployme nt Trust Fund (UTF) for services the Department of the Treasury provided for collecting and processing federal unemployment taxes. The OIG reviewed total administrative charges of $305 million for FYs 1996, 1997, and 1998. The audits showed that Treasury overcharged the UTF $48 million during the audit period because IRS’s estimated costs during this time had not been adjusted to reflect actual costs. The OIG recommended that DOL ensure that IRS credit the UTF for the $48 million overcharged. The report also recommended that DOL establish a team to negotiate an alternative method of charging for IRS administrative costs, since the current method is fragmented, cumbersome, and unreliable. *(DOL)*

OIG Investigation Leads Charitable Organization to Refund $300,000 to AID

A leading charitable organization in Mexico refunded $300,000 in U.S. disaster assistance funds to AID as a result of an AID OIG investigation. The funds had been provided in support of recovery efforts from the effects of Hurricane Pauline. Although the grant agreement required the charitable organization to maintain the AID funds in a separate bank account, it commingled them with other donor funds and was unable to provide a proper accounting of grant expenditures. In addition, the president of the charitable organization donated $200,000 of the AID grant to another organization under the president's control, allegedly in return for medicines. However, the investigation determined that the medicines from the second organization had actually been received as a donation from a non-profit organization in the United States. Further, the medicines received by the original charitable organization could not be accounted for. Finally, there was no evidence that the medicines were substantially received in the areas affected by Hurricane Pauline.

The charitable organization decided to return the grant funding to AID. In lieu of receiving a bill for collection, the charitable organization elected to refund the entire $300,000 immediately, which it did. *(AID)*

OIG Identifies Trends in Fraudulent Use of Social Security Numbers

SSA OIG performed a review to inform SSA officials of trends involving the fraudulent uses of Social Security numbers (SSNs). The report included observations regarding the use of SSNs to commit identity fraud that SSA can use as a catalyst for changes essential to ensuring the integrity of SSA's enumeration responsibility. Recommendations included: 1) policies and performance measures should clearly state that fraud prevention should never be circumvented to satisfy customer-service demands; 2) preventive controls need to be incorporated into the systems database; 3) SSA should require verification from the issuing state when an out-of-state birth certificate is submitted as evidence for an SSN application; and 4) SSA needs to continue efforts to have the Immigration and Naturalization Service (INS) and the Department of State collect and verify enumeration information for aliens.

SSA responded that it plans to issue a reminder to field office personnel regarding the importance of adhering to fraud-prevention procedures, irrespective of customer-service demands. SSA stated that it would work with OIG to target potential fraudulent activity when multiple SSNs are sent to the same address and hoped to obtain online access to state vital records data in the future. SSA also plans to continue its efforts with the INS and DOS for those agencies to collect enumeration information for non-citizens, continue to be vigilant in guarding against fraudulent documents, and continue to work with INS to shorten the verification process. *(SSA)*

FRB Takes Prompt Action After OIG Questions Internal Controls and Expenditures

FRB OIG performed an audit to assess FRB's Academic Assistance program's internal controls, including compliance with applicable laws and regulations. FRB established the program to provide financial assistance to employees taking job-related courses and degree programs, with a dual goal of helping current employees become more knowledgeable and productive and attracting and recruiting new employees.

The OIG found that the program lacked an effective system of internal controls; consequently, FRB had little assurance that the program achieved its goals. The OIG also questioned an estimated $409,000, or slightly more than 50 percent of the academic assistance funds expended during 1997 and through August 1998, because it believes that tax determinations for these amounts may not have been consistent with federal internal revenue laws and regulations. FRB concurred with each of the 10 recommendations and resolved the situations involving taxable income. Management also requested that the OIG advise them on reengineering the program and related business processes to further enhance program integrity, accountability, and results. *(FRB)*

OIG Analyzes Exchanges of Membership Lists with Political Organizations

Reacting to newspaper articles, inquiries from the Congress and top Corporation for Public Broadcasting (CPB) management, CPB OIG performed an expedited review of rentals and/or exchanges of membership/donor lists between public broadcasting stations and political organizations. In a seven-week period, OIG staff conducted a survey of the almost 600 grantees (representing more than 1,000 public broadcasting stations) receiving funding from federal appropriations.

The OIG found that a substantial portion of public broadcasting grantees use direct mail solicitations to obtain nonfederal revenue to help finance their continuing operations. Of the stations that make active use of direct mail, virtually all exchange names with and rent names from a variety of nonprofit organizations. However, only about 10 percent of the stations deal with political organizations. Such transactions represented only a minor role in their direct-mail solicitation process. CPB's board of directors and senior management took prompt action to promulgate eligibility requirements to prohibit such transactions. In November 1999, Congress passed legislation to prohibit stations from receiving CPB grants if they exchange or rent lists with political organizations. *(CPB)*

Cooperative Effort Continues at FCC to Develop Systems Development Review Methodology

At the FCC, OIG auditors worked closely with FCC representatives to develop a systems development review methodology (SDRM). The purpose of the SDRM is to provide a structured process for managing the development of information systems, and for managing systems modification and operation after systems are deployed in the production environment. During FY 1999, OIG auditors co-hosted a series of sessions with representatives from FCC bureaus and offices as well as representatives from FCC's procurement office and Information Technology Center. The primary purpose of these sessions was to finalize the structure of each of the five phases of the SDRM and, within each phase, finalize the language for each section and task. After the structure of each phase is finalized and each section and task is completed, the process will be incorporated into a computer tool that was developed under contract to the OIG. This tool will allow FCC employees to access the SDRM online. *(FCC)*

LSC Uses OIG Audits to Revise Grantee Reporting Guidance

The Legal Services Corporation (LSC) OIG continued its series of audits of case statistical reports in FY 1999. LSC's primary FY 1999 performance plan performance measure is number of clients served. The OIG's audit of FY 1997 grantee data revealed serious overstatements of the number of cases closed. The OIG then conducted audits of FY1998 grantee data. The audits indicated some improvement, but also identified new types of errors.

LSC management used both years' audits to revise reporting guidance to grantees. The Inspector General testified at a House Judiciary Committee oversight hearing in September 1999 on these audit results. The FY 2000 appropriations for LSC requires the OIG to conduct an assessment of the accuracy of 1999 caseload data, and report them to the Appropriations Committees by July 30, 2000. *(LSC)*

OIG Participates in Nationwide Financial Management Teleconference on Single Audit Act

The Appalachian Regional Commission (ARC) OIG continued to place emphasis on helping grant managers prevent and resolve problems. In one such instance, the Development District Association of Appalachia and the Appalachian Regional Commission, in coordination with the ARC OIG, conducted a financial management teleconference focusing on changes to the Single Audit Act and key issues related to grant financial management. The program, which reached about 1,000 program and financial managers and independent public accountants, was broadcast to remote locations in the 13-state Appalachian region and was available nationwide to any organization with capability for obtaining the satellite communication. *(ARC)*

OIG Evaluates FCA Specialization and Certification Programs

FCA OIG reviewed and documented all FCA specialization and certification programs, including their procedures for selecting participants, operating parameters, and associated costs. The OIG surveyed regulated institutions to obtain their views about the credibility of subject-matter specialists developed through these programs. While it found that these programs had generally been successful, the OIG nonetheless offered several recommendations, including: 1) the use of rotational assignments for some programs, 2) service commitments as a condition of participation, 3) cost-benefit analyses to support continuation of the programs, and 4) improving the completeness and reliability of management information in the training database. *(FCA)*

OIG Recommends Improvements in NARA Personal Property Management Program

NARA OIG's review of NARA's personal property management program found that overall, the control of personal property needed improvement. The OIG found that: a) accountability of personal property was not continuous from the time of receipt until disposal; b) the NARA Property Accounting System (PAS) needed improvement, and c) the accountable officer's inventory listings lacked required and reliable information. As a result, the NARA personal property management program did not adequately protect the agency against theft, fraud, waste, abuse, and damage. In addition, the number of items to be included in inventories and the cost of the inventories on hand, and management may have made decisions based on inaccurate data. NARA management agreed with all of OIG's recommended corrective actions. *(NARA)*

OIG Completes Strategic Plan, Institutes Outreach Program in Ongoing GPRA Effort

During FY 1999, NSF OIG finalized its strategic plan, which describes the philosophy guiding its efficiency and integrity activities and its commitment to produce timely, high-quality products useful to customers and stakeholders. The OIG also instituted an outreach program to facilitate constructive dialogue with customers and stakeholders about products, and to identify issues for which assistance would be most useful. Staff members serve as liaisons to each major component of the agency, and meet regularly with division directors to discuss efficiency and integrity matters, as well as other areas of mutual interest.

Along with this informal exchange of information, OIG liaisons regularly brief NSF divisions about the OIG missions and goals, and obtain perspectives from division staff about OIG activities. NSF staff members seek OIG's advice on matters of concern, and have asked OIG to consider new review activities. *(NSF)*

PCC OIG Investigation Reveals Illegal Representation in Claim Against Government

Responding to an allegation, PCC OIG conducted an investigation to determine if a PCC employee acted as an agent or attorney for a government contractor who brought a claim against the U.S. Army. The investigation revealed that a PCC attorney, acting in a non-official capacity, improperly represented a U.S. contractor in a claim against the U.S. Army. At a negotiation meeting, the PCC attorney concealed her true identity by introducing herself and signing the attendance sheet with a false name. During the investigation, she admitted having used a false name and agreed that she should not have accompanied the contractor; however, she denied that she was representing him. Nevertheless, minutes of the meeting provided evidence that the PCC attorney actively participated in the negotiations. Her role had a negative impact on the outcome of the claim.

The OIG presented the case to an assistant U.S. attorney, who declined prosecution since venue and extradition issues make it difficult to prosecute a case involving a foreign (Panamanian) citizen. The OIG recommended that PCC management evaluate the case and initiate appropriate disciplinary action. *(PCC)*

Peace Corps Agrees to Implement All OIG Recommendations in China Audit

The Peace Corps (PC) OIG conducted an audit of the financial and administrative systems of Peace Corps/China. The audit was performed at the post's offices in Chengdu, China, and included visits to volunteers' homes and work locations.

The OIG recommended administrative improvements to enhance current operations and provide for a greater continuity of operations in the future. These included: 1) that advances be carried and reported as outstanding until liquidated, 2) that the billing officer establish an aggressive bill collection and follow-up system, 3) that procurement files document the market analysis conducted before contract award, and 4) that medical items dispensed be recorded in a daily log. The agency concurred with all 15 of the OIG recommendations and all were closed. *(PC)*

SEC Establishes Task Force to Take Action on OIG Recommendations

SEC OIG conducted an audit survey of management's controls for safeguarding sensitive information in the Commission's possession. Types of sensitive information include market-sensitive (e.g., knowledge of unannounced mergers), proprietary (*e.g.,* trading models), business (e.g., customer lists), and information of interest to foreign governments. The survey found that additional controls could significantly enhance the effectiveness of the security of sensitive information. In response, management established a task force to implement corrective actions. *(SEC)*

OIG Supports Procurement Training for TVA Contract Managers/Contract Agents

TVA's procurement office is changing its process for procuring and managing TVA's materials and services. The process will change from a price-focused activity to management of "total cost" throughout the life cycle of the equipment, material, or service. The changes have resulted in the need for a fundamental shift in the role of TVA's traditional purchasing agent, which had primarily been transaction-oriented with a focus on contract management. TVA's contract managers/contract agents (CM/CA) will proactively seek ways to lower total cost and achieve value beyond contract award.

As part of the changing role of CM/CAs, TVA's procurement office developed new, required training, which includes areas such as policies and procedures, strategic outsourcing, solicitations, terms and conditions, and negotiations. In addition to the OIG's ongoing role of conducting pre-award and post-award audits, the OIG also participated in the contract administration training module. In this module, the OIG presented an overview of the audit process and contract fraud awareness. *(TVA)*

OIG Review of Timekeeping Practices Leads ITC to Issue Guidance on Holiday Pay

ITC OIG reviewed ITC's timekeeping practices regarding holidays for employees working compressed work schedules (CWS). The OIG evaluated whether ITC employees on CWS would have been entitled to additional hours for holidays by applying the proper federal rules in lieu of an existing ITC directive and policy.

The OIG found that the ITC's directive and resultant timekeeping practices did not conform to federal statutes and regulations. As a result, the OIG determined that each employee working a CWS was entitled to one to four hours of holiday time for the five holidays reviewed. In total, 142 ITC employees were entitled to 389 additional hours. ITC responded by immediately implementing applicable guidance to calculate holiday hours for employees working CWS. ITC further indicated that it would determine an appropriate remedy to restore past hours for periods not covered by this review. *(ITC)*

OIG Internal Review Reveals Successful Case Control Operation in FLRA

FLRA's IG completed an internal review of FLRA's Case Control Office (CCO). The CCO functions as FLRA's "clerk of the court" and processes incoming cases and outgoing decisions for the members of the Authority. The CCO is also FLRA's point of contact with the public.

The review affirmed a tenured and knowledgeable staff who worked very well together to carry out an institutionalized process with a distinct orientation toward customer service. As part of this review, the IG interviewed customers who had only praise for the CCO teams' interface. Part of the success of the CCO is attributable to its director, who has created a work environment that fosters empowerment, communication, and independence. The review also revealed several areas where positions and workload could be managed more efficiently. In addition, the case-tracking system's data needed more management attention to ensure its validity, as did the area of information security. *(FLRA)*

OIG Helps EEOC Evaluate Effectiveness of FMFIA Processes

EEOC's Office of Research and Information Planning (ORIP) found that the elimination of reporting requirements of the Federal Managers' Financial Integrity Act (FMFIA) in December 1999 presented a timely opportunity to reevaluate the FMFIA process. In support of that objective, the OIG assisted the ORIP in redesigning EEOC's management control system in accordance with FMFIA. The OIG advised ORIP on various methodologies that could help them streamline and improve FMFIA processes, thus making FMFIA a more viable management tool which would aid managers in expeditiously identifying and resolving programmatic concerns. *(EEOC)*

OIG Instrumental in FTC's Decision to Prepare Annual Financial Statements

The OIG was instrumental in FTC's decision to prepare annual financial statements, beginning in FY 1997, consistent with OMB form and content guidance. Even though the agency is not yet required to prepare such statements, the OIG worked with agency financial and program managers to identify the benefits such statements provide to them and to the agency's external customers and stakeholders.

Although the FY 1997 and FY 1998 audits resulted in unqualified opinions, their real value to the agency's program managers was recognized when managers began to use the statements to as a tool to assess the efficiency and effectiveness of agency programs. The Statement of Custodial Activity, the one statement that most distinguishes the FTC from other agencies, provides information on hundreds of millions of dollars of judgments won by the agency on behalf of consumers injured by fraud. It also offers a snapshot of how FTC enforcement programs affect the everyday lives of American consumers. The statements also permit agency managers, for the first time, to use audited numbers to describe the outputs and outcomes of the public's investment in the FTC. For example, the Statement of Net Cost and the Statement of Budgetary Resources show that the agency is largely self-funded due to premerger filing fees collected from parties seeking merger or acquisition approval. *(FTC)*

Committees and Projects

The PCIE, in conjunction with the ECIE, maintains committees to examine important issues and to assist the Councils in their ongoing efforts to improve their members' effectiveness in fighting fraud, waste, and abuse in the federal government.

Audit Committee

In FY 1999, the PCIE Audit Committee continued its leadership role by promoting the following initiatives in the IG community:

- Through its relationship with the Inspector General Auditor Training Institute (IGATI), continued to help identify and provide useful, relevant, and cost-effective training for auditors working in the various IG offices. IGATI enjoyed a record year, recording positive revenues and training over 1,500 students.
- Furthered the effort to adopt, in conjunction with the General Accounting Office, a unified manual providing standard guidance for auditing agency financial statements. The Audit Committee has set as a goal the adoption of a unified manual in time for the audits of the FY 2001 agency financial statements.
- Jointly sponsored, with the Federal Audit Executive Council, a Financial Statement Update Forum for the federal accounting and auditing communities.
- Fostered improved overall audit quality of Single Audit efforts through various initiatives. With the support of the Federal Audit Executive Council, these efforts included the updating and issuance of two review guides to assist the audit community in reviewing A-133 audit reports.
- Encouraged audits and other reviews of cross cutting issues. In this vein, under the leadership of the Department of the Treasury IG, sixteen IGs completed a multi-agency review of non-tax delinquent debt.
- Published a report singling out audit "best practices" of all IGs.
- Reached consensus on a peer review schedule through 2004, by which IGs perform external reviews of the audit functions of their counterpart IGs at other agencies. The new schedule includes assignments for the next two review cycles.
- Formulated and issued a strategic plan containing goals and objectives for the Audit Committee in FY 2000.
- Served as a continuing resource for the audit community.

Investigations Committee

In August 1999, the Investigations Committee presented to the PCIE and the ECIE the results of the Inspector General Criminal Investigator Academy (Academy) study group. At respective meetings, the PCIE and the ECIE voted to implement the recommendations of the study group to consolidate the Academy and the Treasury Inspector General for Tax Administration Training Section. Both training facilities are located at the Federal Law Enforcement Training Center. The other implemented recommendations included having the TIGTA IG as the "Accountable IG" who would be responsible to the Investigations Committee for the overall administration and operation of the Academy. In addition, the Academy would have an executive director located in Washington, DC, to be the primary liaison between the Academy and the IG community, and a director, located at FLETC, to deal with the day-to-day oversight of the Academy.

In September 1999, the Assistant Inspectors General for Investigation and their training officers met for several days and reviewed the current curricula offered at FLETC's Criminal Investigator Training Program, the Academy, and the TIGTA Training Section. They identified duplicative courses and suggested new curricula, ensuring that the final courses offered by the Academy address the needs of the IG community and its special agents.

Legislation Committee

The Legislation Committee ensures that the PCIE is kept abreast of matters in the congressional arena that are of interest to the IG community as a whole, or that could impact OIG statutory authority, duties, and organization as provided under the IG Act. The committee also develops, coordinates, and represents official PCIE positions with regard to particular legislative issues. Additionally, the Committee serves as a resource base for the community on congressional rules, operation, and procedures.

In FY 1999, the committee reviewed 6 pieces of legislation, distributed 19 legislative updates, provided requested comments to OMB on 8 legislative items, and conducted two surveys in response to requests from Congress.

Perhaps the most significant effort of the Legislation Committee, with support from other OIGs, was the consideration of H.R. 1827, the Government Waste Corrections Act of 1999, a bill introduced by Representative Dan Burton, Chairman of the House Committee on Government Reform. The bill seeks to identify and recover, through the practice of "recovery auditing," inadvertent or erroneous overpayments made by federal agencies. Through ongoing discussions with the Committee, OMB, and the CFO Council, the Legislation Committee was able to provide input and suggest modifications to the legislation in several areas. These included Inspector General statutory authority and oversight responsibilities; contractor objectivity and independence; fraud detection, reporting, and referrals; and collection of recovered funds. As a result of these recommendations, the effectiveness of the legislation, now pending before the full House, has been greatly strengthened and enhanced.

Professional Development Committee

In order to meet its responsibilities to provide educational and training opportunities for PCIE and ECIE members, the Professional Development Committee sponsored five forums in FY 1999.

The first forum of FY 1999 focused on GAO/OIG relations. In this forum, members of both communities, including the Acting Comptroller General, spoke about successful relations, historic and current challenges, new opportunities, and specific actions to encourage better collaboration between GAO and the IGs. Several IGs gave presentations, along with GAO area directors, and OIG and GAO congressional liaison officers.

Two presentations were given by Members of Congress: the Honorable Pete Sessions from the Fifth District of Texas and the Honorable Christopher Shays from the Fourth District of Connecticut. Congressman Sessions, a strong advocate for issues that are of importance to the IG community, shared his views on reducing the operating costs of the federal government and reducing waste, fraud and abuse in government operations. He offered to host a meeting of IGs with key Members of Congress and their staffs to exchange ideas and identify ways to promote prudent government management. The meeting was subsequently held in mid-April and resulted in a highly productive discussion of issues. Congressman Shays provided an extensive explanation of the demands and operations of a congressional office.

The Committee also sponsored a presentation by the Department of Justice Office of Inspector General on the Supreme Court decision *National Aeronautics and Space Administration et al. versus the Federal Labor Relations Authority et al.*. This decision affirmed bargaining unit employees' rights to union representation when Office of Inspector General investigators interview agency employees regarding matters that may result in disciplinary or adverse actions. This forum was of particular interest to the community because of its impact on Inspector General operations.

The final forum presented the former Deputy Director of OMB, G. Edward DeSeve. Currently with KPMG Peat Marwick LLP, Mr. DeSeve expressed his thoughts on potential improvements that could be implemented for managing government. He also addressed the importance of Inspectors General in ensuring that necessary steps are taken to improve the efficiency of government.

Inspection and Evaluation Committee

The goals of the PCIE Inspection and Evaluation Committee are: 1) to provide positive contributions to the IG community, as well as the federal government as a whole, in improving the management of federal programs; 2) to improve the practice of inspections and evaluation by sharing effective practices and insights; and 3) to improve the analytic and administrative skills of OIG inspectors and evaluators by providing training in variety of pertinent topics.

The first project the Committee issued this year was an update of the *Survey of Inspection and Evaluation Units in the Inspector General Community*. The original survey was conducted in 1995. Despite changes in the makeup of the evaluation community, inspections and evaluation units seem to be more confident in the kind of evaluative work they perform, the distinct qualities and strengths of their reviews, and how those reviews fit into the overall mission of the OIG. They agree that there are three main ingredients that make these units successful: quality staff, good relationships with their Departments and program managers, and the scope and uniqueness of the work they perform.

Other projects in the early stages of development are:

- *Child Support Enforcement: Ensuring Federal Employees' Compliance* (Wage Withholding and Medical Support). Participating OIGs: Department of Justice, Department of Health and Human Services, and Office of Personnel Management.
- *Federal Department and Agency Processes Dealing with Criminal Computer Penetrations*. Participating OIGs: NASA, Department of Health and Human Services, Small Business Administration, and Department of Justice.

Integrity Committee

The Integrity Committee (IC) receives, reviews, and forwards for further investigation any allegations of wrongdoing by an Inspector General, or, under certain circumstances, OIG staff members.

Complaints

The IC met five times during FY 1999 and reviewed 36 new complaints. Thirty-eight separate complaint matters were processed and brought to closure. These included 19 complaints that the Committee determined were unsubstantiated, frivolous, and/or lacking sufficient details to warrant further action. The IC determined 16 matters to be outside the IC's purview and referred them to other agencies for consideration, and closed two cases after determining that the complaints were substantiated. One matter was closed administratively. The Committee supervised four separate investigations into allegations of misconduct against IGs during FY 1999. Since 1990, the IC has processed and brought to closure 278 cases.

FBI Support

The FBI continues to show its support to the IC by maintaining an appropriate staffing level for the IC's working group. Formerly, the working group consisted of one special agent supervisor, an attorney from the FBI's Office of General Counsel, and one analyst. The working group now includes an additional special agent supervisor, enabling the working group to conduct more in-depth analysis of IC matters, enhance the presentation of cases, expedite the processing of cases, and carry out IC decisions more efficiently and effectively. In addition, recognizing the importance and challenging nature of the IC's work, the FBI authorized an enhancement in the grade level of the working group's analytical position.

Processing Cases Efficiently

The IC now meets bimonthly rather than quarterly, a change necessitated by the increase of IC matters since the signing of the Executive Order. This change has markedly improved the IC's operations by speeding up the Committee's case processing time and making the Committee's actions more timely. In addition, the IC established a 30-day limit when soliciting IGs or complainants for information, which further enhanced the case processing time. While the number of new complaints continues to increase, the time to process these cases has significantly decreased. In 1990, when the IC opened 24 new cases, the average case processing time was 28.7 months. In 1999, when the IC opened 36 new cases, the average case processing time was down to 3.7 months.

STATISTICAL SUMMARIES OF ACCOMPLISHMENTS

Table I-P
PCIE - Recommendations That Funds Be Put To Better Use

Agency	OIG	DCAA	Total
Agency for International Development (AID)	$ 37,403,090	$ 0	$ 37,403,090
Corp. for National and Community Service (CNS)	106,000,000	0	106,000,000
Department of Agriculture (USDA)	274,548,985	103,421	274,652,406
Department of Commerce (DOC)	6,969,710	0	6,969,710
Department of Defense (DoD)	2,727,284,000	3,894,300,000	6,621,584,000
Department of Education (ED)	35,000,000	0	35,000,000
Department of Energy (DOE)	208,855,945	0	208,855,945
Department of Health and Human Services (HHS)[6]	297,763,000	0	297,763,000
Dept. of Housing and Urban Development (HUD)	2,089,000	0	2,089,000
Department of the Interior (DOI) [7]	145,003,304	0	145,003,304
Department of Justice (DOJ)	520,427,693	0	520,427,693
Department of Labor (DOL)	11,847,991	0	11,847,991
Department of State (DOS)[8]	500,000	0	500,000
Department of Transportation (DOT)	1,002,348,000	0	1,002,348,000
Department of the Treasury (Treasury)	73,994,000	5,062,000	79,056,000
Department of Veterans Affairs (VA)	643,380,000	15,920,000	659,300,000
Environmental Protection Agency (EPA)	95,115	1,657,518	1,752,633
Federal Deposit Insurance Corporation (FDIC) [9]	10,308,806	0	10,308,806
Federal Emergency Management Agency (FEMA)	2,802,451	0	2,802,451
General Services Administration (GSA)	362,686,203	0	362,686,203
National Aeronautics and Space Admin (NASA)[10]	49,350,000	60,824,000	110,174,000
Nuclear Regulatory Commission (NRC)	0	0	0
Office of Personnel Management (OPM)	0	0	0
Railroad Retirement Board (RRB)	59,133,850	0	59,133,850
Small Business Administration (SBA)	753,086	0	753,086
Social Security Administration (SSA)[11]	519,716,442	0	519,716,442
Treasury IG for Tax Administration (TIGTA)	191,202,000	0	191,202,000
United States Information Agency (USIA)	1,001,000	0	1,001,000
TOTALS	**$ 7,290,463,671**	**$ 3,977,866,939**	**$ 11,268,330,610**

[6] Figures include the results of HHS OIG inspections.

[7] Includes funds of $50 million attributable to lost revenues, such as the value of uncollectable, defaulted loans. Also includes net adjustments of $9,730,798 to indirect cost proposals negotiated by the DOI/OIG with Indian tribal and state and local governments which resulted in decreases to the indirect cost rates.

[8] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[9] Figures include two evaluation reports, totaling $6,743,806.

[10] Figures include the results of NASA OIG inspections.

[11] The amounts include a $250,000,000 cost avoidance that is realized annually (from 1995 to 2001) as a result of two audit reports: “Effectiveness of Obtaining Records to Identify Prisoners” and “Effectiveness of the Social Security Administration’s Procedures to Process Prisoner Information, Suspend Payments and Collect Overpayments.”

Table I-E

ECIE - Recommendations That Funds Be Put To Better Use

Entity	Total
Amtrak	$ 677,599
Appalachian Regional Commission (ARC)	2,230,000
Commodity Futures Trading Commission (CFTC)	0
Consumer Product Safety Commission (CPSC)	0
Corporation for Public Broadcasting (CPB)	0
Equal Employment Opportunity Commission (EEOC)	0
Farm Credit Administration (FCA)	0
Federal Communications Commission (FCC)	0
Federal Election Commission (FEC)	0
Federal Housing Finance Board (FHFB)	0
Federal Labor Relations Authority (FLRA)	0
Federal Maritime Commission (FMC)	0
Federal Reserve Board (FRB)	0
Federal Trade Commission (FTC)	222,000
Government Printing Office (GPO)	561
International Trade Commission (ITC)	0
Legal Services Corporation (LSC)	0
National Archives and Records Administration (NARA)	355
National Credit Union Administration (NCUA)	0
National Endowment for the Arts (NEA)	0
National Endowment for the Humanities (NEH)	0
National Labor Relations Board (NLRB)	0
National Science Foundation (NSF)	6,213,604
Panama Canal Commission (PCC)	0
Peace Corps (PC)	30,000
Pension Benefit Guaranty Corporation (PBGC)	0
Securities and Exchange Commission (SEC)	0
Smithsonian Institution (SI)	0
Tennessee Valley Authority (TVA)	11,262,570
U.S. Postal Service (USPS)[12]	1,259,690,973
TOTAL	**$ 1,280,327,662**

[12] Amount includes $962 million in potential cost avoidance for the Corporate Call Management Program through FY 2007.

Table II-P

PCIE - MANAGEMENT DECISIONS ON RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE

Agency	No Management Decision Start FY 1999	Recommendations Issued in FY 1999	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 1999
AID[13]	$ 484,949,143	$ 37,403,090	$ 194,614,107	$ 313,885,729	$ 14,049,538
CNS	1,609,000	106,000,000	107,609,000	0	0
DOC[14]	22,031,128	6,969,710	9,267,868	1,120,896	18,631,904
DoD[15]	11,481,900,000	6,621,584,000	2,975,087,000	3,962,397,000	11,173,900,000
DOE	443,375,886	208,855,945	24,987,250	221,150,421	406,094,160
DOI	340,039,557	145,003,304	97,310,040	7,376,771	380,356,050
DOJ	32,000,242	520,427,693	548,163,213	127,974	4,136,748
DOL	7,546,356	11,847,991	12,114,649	475,000	6,804,698
DOS[16]	7,346,000	500,000	7,500,000	0	346,000
DOT	407,996,000	1,002,348,000	676,386,000	53,726,000	680,232,000
ED	18,191,552	35,000,000	0	3,891,552	49,300,000
EPA[17]	0	1,752,633	1,657,518	0	95,115
FDIC[18]	0	10,308,806	10,308,806	0	0
FEMA	191,991,585	2,802,451	150,740,516	1,075,062	42,978,458
GSA[19]	251,211,250	361,883,958	401,054,099	193,618,329	18,252,239
HHS[20]	1,451,106,000	297,763,000	312,748,000	175,000	1,435,946,000
HUD	4,367,000	2,089,000	463,000	385,000	5,608,000
NASA[21]	6,058,030,198	110,174,000	33,799,000	5,577,501,198	556,904,000
NRC	0	0	0	0	0
OPM	0	0	0	0	0
RRB	0	59,133,850	59,133,850	0	0
SBA[22]	18,947,417	753,086	8,929,983	488,675	10,441,023
SSA[23]	0	519,716,442	250,000,000	0	269,716,442
Treasury	73,605,000	79,056,000	42,942,000	49,647,000	60,072,000
TIGTA	0	191,202,000	191,202,000	0	0
USDA[24]	108,611,953	274,652,406	114,086,281	15,992,601	253,312,909
USIA	100,000	1,001,000	0	0	1,101,000
VA	245,400,000	659,300,000	655,400,000	133,100,000	116,200,000
TOTALS[25]	**$ 21,650,355,267**	**$ 11,267,528,365**	**$ 6,885,504,180**	**$ 10,536,134,208**	**$ 15,496,245,244**

[13] The beginning balance for FY 1999 reflects an increase of $227,192 over the ending balance for FY 1998 that appeared in last year's report. This increase consists of: 1) an adjustment of $30,051 in one report, and 2) a recommendation in another report that was increased by $197,141.

[14] Management agreed to funds to be put to better use that exceeded recommended amounts by $19,830.

[15] Reflects a variance of $664,504,000 between the end of FY 1998 and the beginning of FY 1999 balances due to contracts not awarded and revised audit findings and recommendations.

[16] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[17] Any difference in amounts between FY 1999 beginning figures and FY 1998 ending figures results from corrections made to data in EPA/OIG's tracking system.

[18] Figures include two evaluation reports, totaling $6,743,806.

[19] The difference between the amount in the "Recommendations Issued" column in this table and that in the "Total" column in Table I-P represents recommendations in a final report removed from the resolution process pending litigation.

[20] Opening balance adjusted for amended disallowances resulting from Departmental Appeals Board decisions, Department of Justice action, etc.

[21] NASA OIG changed its reporting procedure beginning in FY 1999. Monetary benefits are reported when a management decision has been made for all monetary benefits associated with a report, not on each recommendation. Consequently, the "No Mgmt. Decision End FY 1998" from the FY 1998 Progress Report and the "No Mgmt. Decision Start FY 1999" from this table do not match.

[22] Management agreed to $159,178 more than recommended.

[23] The amounts include a $250,000,000 cost avoidance that is realized annually (from 1995 to 2001) as a result of two audit reports: "Effectiveness of Obtaining Records to Identify Prisoners" and "Effectiveness of the Social Security Administration's Procedures to Process Prisoner Information, Suspend Payments and Collect Overpayments."

[24] Beginning balance increase of $853,916 over ending balance for FY 1998 reflects adjustment made after semiannual period. End column reflects a variance of $127,432 between beginning and ending balances because of inclusion of excess amounts and adjustments in management decisions.

[25] Totals do not crossfoot because of variances reflected in footnotes.

Table II-E

ECIE – Management Decisions on Recommendations That Funds Be Put To Better Use

Entity	No Management Decision Start FY 1999	Recommendations Issued in FY 1999	Recommendations Agreed to By Management	Recommendations Not Agreed to By Management.	No Management Decision End FY 1999
Amtrak	$ 137,073	$ 677,599	$ 365,131	$ 137,073	$ 312,468
ARC	300,000	2,230,000	1,094,000	747,000	689,000
CFTC	0	0	0	0	0
CPB	70,000	0	0	0	70,000
CPSC	0	0	0	0	0
EEOC	0	0	0	0	0
FCA	0	0	0	0	0
FCC	0	0	0	0	0
FEC	0	0	0	0	0
FHFB	0	0	0	0	0
FLRA	0	0	0	0	0
FMC	0	0	0	0	0
FRB	0	0	0	0	0
FTC	0	222,000	222,000	0	0
GPO	561	0	0	561	0
ITC	0	0	0	0	0
LSC	0	0	0	0	0
NARA	0	355	0	355	0
NCUA	0	0	0	0	0
NEA	0	0	0	0	0
NEH	0	0	0	0	0
NLRB	0	0	0	0	0
NSF	6,540,411	6,213,604	8,137,403	120,722	4,495,890
PBGC	0	0	0	0	0
PC	0	0	0	0	0
PCC	0	0	0	0	0
SEC	0	0	0	0	0
SI	273,318	0	238,309	35,009	0
TVA	0	11,262,570	8,592,641	1,880,919	789,010
USPS	172,746,838	1,259,690,973	1,328,268,958	0	104,168,853
TOTALS	**$ 180,068,200**	**$ 1,280,297,100**	**$ 1,346,918,442**	**$ 2,921,639**	**$ 110,525,221**

Table III-P

PCIE – QUESTIONED COSTS[26]

Agency	OIG	DCAA	Total
AID	$ 31,266,570	$ 10,191,642	$ 41,458,212
CNS	2,344,000	0	2,344,000
DOC	5,610,639	0	5,610,639
DoD[27]	0	2,935,900,000	2,935,900,000
DOE	971,560	0	971,560
DOI	32,019,252	2,971,812	34,991,064
DOJ	25,469,588	0	25,469,588
DOL	65,154,720	0	65,154,720
DOS[28]	642,000	377,992	1,019,992
DOT	13,659,000	0	13,659,000
ED	69,804,793	0	69,804,793
EPA	76,679,839	2,570,733	79,250,572
FDIC	8,100,242	0	8,100,242
FEMA[29]	28,519,506	0	28,519,506
GSA	26,331,335	0	26,331,335
HHS	212,066,771	3,229	212,070,000
HUD	24,208,000	0	24,208,000
NASA[30]	70,914,734	66,651,000	137,565,734
NRC	0	485,853	485,853
OPM	95,109,139	0	95,109,139
RRB	0	0	0
SBA	2,317,050	0	2,317,050
SSA	83,989,044	0	83,989,044
Treasury	0	3,937,000	3,937,000
TIGTA	490,000	325,075	815,075
USDA[31]	118,411,914	1,233,845	119,645,759
USIA	6,089,000	0	6,089,000
VA	10,293,769	0	10,293,769
TOTALS	**$ 1,010,462,465**	**$ 3,024,648,181**	**$ 4,035,110,646**

1

[26] Includes unsupported costs unless otherwise noted.

[27] Opening balance reflects a variance of $664,504,000 between the end of FY 1998 and the beginning of FY 1999 balances due to contracts not awarded and revised audit findings and recommendations.

[28] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[29] Non-FEMA auditors (other than DCAA) questioned $1,187,929. FEMA is tracking this amount in its Audit Follow-up System.

[30] NASA/OIG changed its reporting procedure beginning in FY 1999. Monetary benefits are reported when a management decision has been made for all monetary benefits associated with a report, not on each recommendation. Consequently, the "No Mgmt. Decision End FY 1998" from the Fiscal Year 1998 Progress Report and the "No Mgmt. Decision Start FY 1999" from this table do not match. Also, the amount includes $59,000,000 in questioned costs from investigations.

[31] Includes $73,898 in recommendations from work performed by non-federal auditors.

Table III-E

ECIE - QUESTIONED COSTS[32]

Entity	Costs Questioned by OIG	Costs Questioned by DCAA	Total
Amtrak	$ 30,341,954	$ 0	$ 30,341,954
ARC	78,000	0	78,000
CFTC	0	0	0
CPB	109,969	0	109,969
CPSC	0	0	0
EEOC	0	0	0
FCA	31,892	0	31,892
FCC	719,118	0	719,118
FEC	0	0	0
FHFB	0	0	0
FLRA	0	0	0
FMC	0	0	0
FRB	409,000	0	409,000
FTC	0	0	0
GPO	63,816	0	63,816
ITC	0	0	0
LSC	0	0	0
NARA	0	2,805	2,805
NCUA	0	0	0
NEA	176,414	0	176,414
NEH	0	0	0
NLRB	0	0	0
NSF	5,180,932	250,397	5,431,329
PBGC	0	0	0
PC	8,617	0	8,617
PCC	415,861	0	415,861
SEC	0	0	0
SI	0	0	0
TVA	2,815,221	0	2,815,221
USPS	31,938,680	0	31,938,680
TOTAL	**$ 72,289,474**	**$ 253,202**	**$ 72,542,676**

[32] Includes unsupported costs unless otherwise noted.

Table IV-P
PCIE - MANAGEMENT DECISIONS ON AUDITS WITH QUESTIONED COSTS[33]

Agency	No Management Decision Start FY 1999	Recommendations Issued in FY 1999	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 1999
AID[34]	$ 18,477,917	$ 41,458,212	$ 23,005,638	$ 15,056,160	$ 21,874,331
CNS	1,803,000	2,344,000	273,000	991,000	2,883,000
DOC[35]	8,426,122	5,610,639	5,154,868	7,085,121	2,038,460
DoD[36]	6,965,800,000	2,935,900,000	1,159,900,000	778,800,000	7,963,000,000
DOE[37]	7,759,186	826,624	1,524,891	631,366	6,552,760
DOI	178,206,569	32,019,252	11,573,316	3,990,321	194,662,184
DOJ	48,228,184	25,469,588	61,282,178	213,433	12,202,161
DOL	47,154,478	65,154,720	20,200,859	7,635,647	84,472,692
DOS[38]	145,000	642,000	0	4,000	783,000
DOT	7,116,000	13,659,000	5,630,000	9,516,000	5,629,000
ED	107,426,745	69,804,793	4,148,668	4,626,846	168,454,367
EPA[39]	112,446,837	79,250,572	41,392,156	52,778,011	97,527,242
FDIC[40]	727,945	8,100,242	6,760,918	2,099,224	0
FEMA	35,527,858	28,519,506	30,306,379	4,219,832	29,521,153
GSA[41]	7,335,241	26,331,335	28,641,446	1,542,743	3,789,108
HHS[42]	281,712,000	212,070,000	251,499,000	14,174,000	228,109,000
HUD	32,305,000	24,208,000	32,834,000	2,635,000	21,044,000
NASA[43]	202,404,105	137,565,734	36,565,838	28,921,319	274,482,682
NRC	0	485,853	485,853	0	0
OPM	28,252,890	95,109,139	49,485,555	17,788,174	56,088,300
RRB	0	0	0	0	0
SBA	2,997,662	2,317,050	2,317,780	1,204,667	1,792,265
SSA	390,187	83,989,044	4,955,581	0	79,423,650
Treasury	13,410,000	3,937,000	8,116,000	4,312,000	4,919,000
TIGTA	0	815,075	490,000	0	325,075
USDA[44]	414,443,028	119,645,759	262,521,105	26,021,959	246,746,433
USIA	3,165,000	6,092,000	0	2,352,000	6,905,000
VA	0	10,300,000	10,300,000	0	0
TOTALS	**$ 8,525,662,953**	**$ 4,031,625,136**	**$ 2,059,365,029**	**$ 986,598,823**	**$ 9,513,226,862**

[33] Includes unsupported costs unless otherwise noted.

[34] The beginning balance for FY 1999 was decreased from the ending balance for FY 1998 by $1,249,841. This adjustment reflects an increase of $51,220 for one report and a rescission of recommendations in several reports totaling $1,301,061.

[35] Management agreed to questioned costs that exceeded the recommended amounts by $241,688.

[36] Opening balance reflects a variance of $897,543,000 between the end of FY 1998 and the beginning of FY 1999 balances due to contracts not awarded and revised audit findings and recommendations.

[37] Beginning balance of $7,759,186 does not include $84,241 of unsupported costs. The amount $826,624 in the “Recommendations Issued” column does not include $60,695 of unsupported costs discovered during FY 1999. The figure $6,552,760 in the “No Mgmt. Decision” column does not include unsupported costs of $144,936.

[38] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[39] Differences in amounts between FY 1999 beginning figures and FY 1998 ending figures result from corrections made to data in OIG’s tracking system.

[40] Includes FDIC management disallowance of $5,816 more than questioned, and a revised management decision to disallow $26,139 from a recommendation issued during the previous Fiscal Year.

[41] Amount in “Recommendations Agreed to” column includes $306,721 that management agreed to seek that exceeded the recommended amounts.

[42] Opening balance adjusted for a revaluation of savings estimates.

[43] NASA OIG changed its reporting procedure beginning in FY 1999. Monetary benefits are reported when a management decision has been made for all monetary benefits associated with a report, not on each recommendation. Consequently, the “No Mgmt. Decision End FY 1998” from the FY 1998 Progress Report and the “No Mgmt. Decision Start FY 1999” from this table do not match.

[44] Beginning balance increase of $511,730 over ending balance for FY 1998 reflects adjustment made after semiannual period. Amounts in columns 2 and 6 reflect a variance of $1,200,710 because of inclusion of excess amounts and adjustments in management decisions.

Table IV-E

ECIE - Management Decisions on Audits with Questioned Costs[45]

Entity	No Management Decision Start FY 1999	Recommendations Issued In FY 1999	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 1999
Amtrak	$ 2,496,629	$ 30,341,954	$ 27,960,278	$ 980,858	$ 3,897,447
ARC	1,009,000	78,000	351,000	659,000	77,000
CFTC	0	0	0	0	0
CPB	158,450	109,969	0	0	268,419
CPSC	0	0	0	0	0
EEOC	0	0	0	0	0
FCA	31,892	0	31,892	0	0
FCC	265,180	719,118	717,976	1,142	265,180
FEC	0	0	0	0	0
FHFB	0	0	0	0	0
FLRA	0	0	0	0	0
FMC	0	0	0	0	0
FRB	0	409,000	409,000	0	0
FTC	0	0	0	0	0
GPO	101,904	63,816	7,008	158,712	0
ITC	0	0	0	0	0
LSC	0	0	0	0	0
NARA	0	2,805	0	0	2,805
NCUA	0	0	0	0	0
NEA	0	176,414	10,300	166,114	0
NEH	0	0	0	0	0
NLRB	0	0	0	0	0
NSF	10,638,622	5,431,329	3,677,315	7,345,581	5,047,055
PBGC	0	0	0	0	0
PC	0	0	0	0	0
PCC	738,665	415,861	221,896	423,069	509,561
SEC	0	0	0	0	0
SI	1,100,878	0	1,089,175	11,703	0
TVA	44,668	2,815,221	1,663,239	61,748	1,134,902
USPS	161,989,656	31,938,680	162,365,497	7,116,023	24,446,816
TOTALS	**$ 178,575,543**	**$ 72,502,166**	**$ 198,504,576**	**$ 16,923,950**	**$ 35,681,184**

[45] Includes unsupported costs unless otherwise noted.

Tables V through IX illustrate the results obtained through OIG investigations during FY 1999. They summarize the statistical accomplishments reported to the Congress as of March 31 and September 30, 1999. These accomplishments — successful criminal prosecutions, administrative sanctions, and investigative and civil recoveries — include the results of joint investigations.

During FY 1999, PCIE OIG investigations resulted in 3,704 successful criminal prosecutions; ECIE OIG investigations resulted in 9,360 successful criminal prosecutions, of which the U.S. Postal Service accomplished 9,337. During FY 1999, PCIE OIG investigations resulted in 798 personnel actions; ECIE OIG investigations resulted in 275 personnel actions.

PCIE OIG investigations resulted in 6,660 suspensions or debarments during FY 1999, and ECIE OIG investigations resulted in 22 suspensions or debarments. During FY 1999 PCIE OIG investigations resulted in about $1.7 billion in recoveries; ECIE OIG investigations resulted in about $60 million in recoveries.

Table V
PCIE AND ECIE
SUCCESSFUL CRIMINAL PROSECUTIONS

PCIE		ECIE	
Agency	**Total**	**Entity**	**Total**
AID	2	Amtrak	0
CNS	2	ARC	1
DOC	6	CFTC	0
DoD	310	CPSC	0
DOE	11	CPB	1
DOI	30	EEOC	1
DOJ	137	FCA	0
DOL	330	FCC	0
DOS	19	FEC	0
DOT	164	FHFB	0
ED	52	FLRA	0
EPA	12	FMC	0
FDIC	21	FRB	0
FEMA	32	FTC	0
GSA	15	GPO	1
HHS	401	ITC	0
HUD	72	LSC	0
NASA	46	NARA	0
NRC	0	NCUA	0
OPM	14	NEA	0
RRB	79	NEH	0
SBA	53	NLRB	0
SSA	960	NSF	3
Treasury	7	PBGC	1
TIGTA	230	PCC	0
USDA	559	PC	0
USIA[46]	0	SEC	0
VA	140	SI	1
		TVA	14
		USPS[47]	9,337
SUBTOTAL	**3,704**	**SUBTOTAL**	**9,360**
	TOTAL	**13,064**	

[46] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[47] Of the total 9,337 prosecutions, 9,330 resulted from Postal Inspection Service investigations and 7 from investigations by the OIG.

Table VI

PCIE AND ECIE — CIVIL ACTIONS

PCIE		ECIE	
Agency	Total	Entity	Total
AID	17	Amtrak	0
CNS	0	ARC	0
DOC	5	CFTC	0
DoD	143	CPB	0
DOE	8	CPSCB	0
DOI	6	EEOC	0
DOJ	2	FCA	0
DOL	86	FCC	0
DOS[48]	0	FEC	26
DOT	0	FHFB	0
ED	92	FMC	0
EPA	2	FRB	0
FDIC	15	FRB	0
FEMA	4	FTO	0
GSA	13	GPO	0
HHS	541	ITC	0
HUD	11	LSC	0
NASA	3	NARA	0
NRC	0	NCUA	0
OPM	1	NEA	0
RRB	50	NEH	0
SBA	9	NLRB	0
SSA	8	NSF	3
Treasury	0	PBGC	0
TIGTA	0	PCC	0
USDA	116	PC	0
USIA	0	SEC	0
VA	61	SI	0
		TVA	2
		USPS	0
SUBTOTAL	**1,193**	**SUBTOTAL**	**31**
	TOTAL	**1,224**	

Civil Actions: include the total number of matters arising from OIG investigations, audits, and other reviews, other than criminal prosecutions, that are successfully resolved during the year. The term includes civil judgments and settlements, and administratively imposed penalties and assessments (such as under the Program Fraud Civil Remedies Act or Civil Monetary Penalties Law). Note that resolutions of personnel actions and debarments/exclusions are covered in other tables and are not reported as Civil Actions.

[48] Includes Arms Control and Disarmament Agency and Broadcasting Board of Governors, both of which reported 0 civil actions.

Table VII

PCIE and ECIE – Personnel Actions

PCIE		ECIE	
Agency	**Total**	**Entity**	**Total**
AID	15	Amtrak	0
CNS	6	ARC	0
DOC	9	CFTC	0
DoD	121	CPSC	0
DOE	27[49]	CPB	0
DOI	27	EEOC	1
DOJ	64	FCA	0
DOL	38	FCC	0
DOS[50]	21	FEC	0
DOT	30	FHFB	0
ED	0	FLRA	0
EPA	12	FMC	0
FDIC	6	FRB	5
FEMA	8	FTC	6
GSA	11	GPO	26
HHS	1	ITC	13
HUD	4	LSC	2
NASA	25	NARA	2
NRC	43	NCUA	1
OPM	1	NEA	0
RRB	0	NEH	0
SBA	8	NLRB	6
SSA	40	NSF	9
Treasury	13	PBGC	1
TIGTA	310	PCC	21
USDA	65	PC	0
USIA	5	SEC	4
VA	39	SI	2
		TVA	15
		USPS	161
SUBTOTAL	**949**	**SUBTOTAL**	**275**
	TOTAL	**1,224**	

Personnel Actions: the total number of reprimands, suspensions, demotions, or terminations of federal, state, and local (including federal contractor/grantee) employees resulting from OIG work or subsequent actions.

[49] Includes 2 personnel actions that DOE took based on Office of Inspections work from the first half of the fiscal year.

[50] Includes Arms Control and Disarmament Agency (ACDA) with 0 and Broadcasting Board of Governors (BBG) with 1 personnel action.

Table VIII
PCIE AND ECIE – SUSPENSIONS/DEBARMENTS

PCIE		ECIE	
Agency	**Total**	**Entity**	**Total**
AID	4	Amtrak	0
CNS	0	ARC	0
DOC	0	CFTC	0
DoD	310	CPB	0
DOE	17	CPSC	0
DOI	0	EEOC	0
DOJ	0	FCA	0
DOL	0	FCC	0
DOS[51]	0	FEC	0
DOT	16	FHFB	0
ED	1	FLRA	0
EPA	11	FMC	0
FDIC	0	FRB	0
FEMA	0	FTC	0
GSA	57	GPO	17
HHS	2,976	ITC	0
HUD	83	LSC	0
NASA	16	NARA	0
NRC	0	NCUA	0
OPM	2,743	NEA	0
RRB	0	NEH	0
SBA	3	NLRB	0
SSA	0	NSF	3
Treasury	0	PBGC	0
TIGTA	N/A[52]	PCC	0
USDA	409	PC	0
USIA	0	SEC	0
VA	14	SI	0
		TVA	0
		USPS	2
SUBTOTAL	**6,660**	**SUBTOTAL**	**22**
	TOTAL	**6,682**	

Suspensions/Debarments: the total number of individuals and entities, including contractors, grantees, and assistance recipients, restricted from doing business with the federal government.

[51] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG), with 0 in all columns.

[52] Data not available.

Table IX
PCIE and ECIE – Investigative Recoveries

PCIE		ECIE	
Agency	**Total**	**Entity**	**Total**
AID	$ 705,619	Amtrak	$ 0
CNS	142,634	ARC	0
DOC	124,198	BBG	2,320
DoD	935,810,188	CFTC	0
DOE	13,618,731	CPSC	0
DOI	14,732,036	CPB	29,000
DOJ	2,237,321	EEOC	3,200
DOL	47,301,997	FCA	0
DOS[53]	754,657	FCC	0
DOT	24,253,605	FEC	0
ED	10,633,798	FHFB	0
EPA	673,868	FLRA	0
FDIC	16,279,357	FMC	0
FEMA	3,040,000	FRB	12,145[54]
GSA	12,900,875	FTC	0
HHS	407,700,000	GPO	165,585
HUD	6,713,196	ITC	0
NASA	40,900,000	LSC	0
NRC	28,366	NARA	0
OPM	2,360,905	NCUA	0
RRB	2,522,620	NEA	0
SBA	10,419,102	NEH	0
SSA	40,271,097	NLRB	177,645
Treasury	707,674	NSF	815,856
TIGTA	25,123,577	PBGC	52,172
USDA	59,480,044	PCC	69,236
USIA	42,561	PC	0
VA	24,295,831	SEC	0
		SI	0
		TVA	2,960,968[55]
		USPS	56,997,125
SUBTOTAL	**$ 1,703,773,857**	**SUBTOTAL**	**$61,285,252**
TOTAL		**$ 1,765,059,109**	

[53] Includes Arms Control and Disarmament Agency (ACDA) with 0 and Broadcasting Board of Governors (BBG), with $2,320.

[54] The dollar figure shows amounts returned to the Federal Reserve Board. The major source of Federal Reserve income is earnings on the portfolio of U.S. government securities in the System Open Market Account. Earnings in excess of expenses, dividends, and surpluses are transferred to the U.S. Treasury. By reducing expenses, these collections are indirectly returned to the U.S. Treasury.

[55] This figure is $10,000 more than the recoveries reported in TVA/OIG's semiannual reports for FY 1999. A $10,000 fine inadvertently was not recorded as an investigative recovery.

Table X

PCIE and ECIE – Collections from Audits and Investigations

The data in this table represent the total amount of funds returned to the Department of the Treasury or the Department of Justice during FY 1999 as a result of OIG audits and investigations during FY 1999 or previous fiscal years. For some agencies and entities, this data is not available or not applicable (N/A).

PCIE			ECIE		
Agency	**From Audi ts**	**From Investigations**	**Entity**	**From Audits**	**From Investigations**
AID[56]	$ 10,496,000	$ 586,494	Amtrak	$ 0	$ 0
CNS	N/A	N/A	ARC	0	0
DOC	N/A	N/A	CFTC	0	0
DoD	N/A	N/A	CPSC	0	0
DOE[57]	N/A	N/A	CPB	0	0
DOI	N/A	N/A	EEOC	0	0
DOJ[58]	0	338,880	FCA	0	0
DOL	7,172,112	941,026	FCC	37,492	0
DOS[59]	0	0	FEC	0	0
DOT	0	2,765,765	FHFB	0	0
ED	1,691,370	8,660,333	FLRA	614	0
EPA	N/A	N/A	FMC	0	0
FDIC	0	N/A	FRB	0	12,145
FEMA	31,105,231	1,033,000	FTC	0	0
GSA	0	0	GPO	0	165,585
HHS	165,354,844	271,335,629	ITC	0	0
HUD	20,223,000	213,357	LSC	0	0
NASA	305,000	2,237,497	NARA	0	0
NRC	0	0	NCUA	0	0
OPM	N/A	N/A	NEA	1,189	0
RRB	0	855,655	NEH	0	0
SBA	1,505,947	121,002	NLRB	0	177,000
SSA	21,079,322	3,453,264	NSF	1,402,618	150,000
Treasury	0	0	PBGC	0	195
TIGTA[60]	0	817,316	PCC	0	0
USDA[61]	31,280,771	10,827,184	PC	0	0
USIA	0	0	SEC	0	0
VA	240,000	17,480,798	SI	0	0
	0	0	TVA	0	58,833
	0	0	USPS	0	0
SUBTOTAL	**$ 290,453,597**	**$ 321,667,200**	**SUBTOTAL**	**$ 1,441,913**	**$ 563,758**
Total Audit PCIE/ECIE	**$291,895,510**		**Total Investigation PCIE/ECIE**	**$322,230,958**	

[56] Source: agency management

[57] The DOE/OIG does not track actual funds returned to the Department of the Treasury or the Department of Justice. It tracks only court-ordered and management-ordered fines, restitutions, and settlements.

[58] The investigations amount represents bribe monies deposited to the Treasury.

[59] Includes Arms Control and Disarmament Agency (ACDA) and Broadcasting Board of Governors (BBG) with 0 in all columns.

[60] TIGTA does not track actual IRS collections that result from audit recommendations. The investigations amount includes federal income tax collected as a result of TIGTA investigation.

[61] Unless otherwise provided by law, monies collected are returned to Treasury.

The President's Council on Integrity and Efficiency
Membership Addresses and Hotline Numbers

Sally Katzen, Acting Chair*
Counselor to the Director
Office of Management and Budget
17th and Pennsylvania Ave., NW
Room 260, Eisenhower EOB
Washington, DC 20503

Gaston L. Gianni, Jr., Vice Chair, PCIE*
Inspector General
Federal Deposit Insurance Corporation
801 17TH Street, NW, Room 1096
Washington, DC 20434-0001
☎800-964-3342

Barry R. Snyder, Vice Chair, ECIE*
Inspector General
Federal Reserve Board
Mail Stop 300
20th Street and Constitution Avenue, NW
Washington, DC 20551
☎800-827-3340 or 202-452-6400

Everett Mosley, Acting Inspector General
Agency for International Development
Ronald Reagan Building, Room 6.6D
1300 Pennsylvania Avenue, NW
Washington, DC 20523
☎800-230-6539 or 202-712-1023

Roger C. Viadero, Inspector General
Department of Agriculture
1400 Independence Ave., SW
Room 117-W Whitten Building
Washington, DC 20250-2301
☎800-424-9121 or 202-690-1622

L. Britt Snider, Inspector General
Central Intelligence Agency
Room 2X30, New Headquarters
Washington, DC 20505

Johnnie Frazier, Inspector General
Department of Commerce
14th & Constitution Ave., NW, Room 7898C
Washington, DC 20230
☎800-424-5197 or 202-482-2495

Luise S. Jordan, Inspector General
Corporation for National Service
1201 New York Ave., NW, Suite 8100
Washington, DC 20525
☎800-452-8210

Donald Mancuso, Acting Inspector General
Department of Defense
400 Army Navy Drive, Room 1000
Arlington, VA 22202-2884
☎800-424-9098 or 703-604-8546

Lorraine Lewis, Inspector General
Department of Education
400 Maryland Ave., SW, Room 4006 MES
Washington, DC 20202-1510
☎800-647-8733 or 202-205-5770

Gregory H. Friedman, Inspector General
Department of Energy
1000 Independence Ave., SW, Room 5D-039
Washington, DC 20585
☎800-541-1625 or 202-586-4073

Nikki L. Tinsley, Inspector General
Environmental Protection Agency
401 M Street, SW, Room NE3309 (2410)
Washington, DC 20460
☎202-260-4977 or 888-565-8740

Ruben Garcia, Jr., Assistant Director*
Criminal Investigative Division
Federal Bureau of Investigation
935 Pennsylvania Ave., NW, Room 7116
Washington, DC 20535

George J. Opfer, Inspector General
Federal Emergency Management Agency
500 C Street, SW, Suite 505
Washington, DC 20472
☎800-323-8603

William R. Barton, Inspector General
General Services Administration
18th & F Streets, NW, Room 5340
Washington, DC 20405
☎800-424-5210 or 202-501-1780

Stephen D. Potts, Director*
Office of Government Ethics
1201 New York Avenue, NW, Suite 500
Washington, DC 20005-3917

June Gibbs Brown, Inspector General
Department of Health & Human Services
330 Independence Ave., SW, Room 5250
Washington, DC 20201
☎800-447-8477

Susan Gaffney, Inspector General
Department of Housing & Urban Devel.
451 7th Street, SW, Room 8256
Washington, DC 20410-4500
☎800-347-3735 or 202-708-4200

Earl E. Devaney, Inspector General
Department of the Interior
1849 C Street, NW, Mail Stop 5341
Washington, DC 20240
☎800-424-5081 or 202-208-5300

Robert L. Ashbaugh, Acting Inspector General
Department of Justice
950 Pennsylvania Ave., NW, Room 4706
Washington,. DC 20530
☎800-869-4499

Patricia Dalton, Acting Inspector General
Department of Labor
200 Constitution Ave., NW, Room S-1301
Washington, DC 20210
☎800-347-3756 or 202-219-5227

Roberta L. Gross, Inspector General
National Aeronautics & Space Admin.
300 E Street, SW, Code W, Room 8T79
Washington, DC 20546
☎800-424-9183

Hubert T. Bell, Inspector General
Nuclear Regulatory Commission
Mail Stop T5 D28
Washington, DC 20555
☎800-233-3497

John U. Sepulveda, Deputy Director*
Office of Personnel Management
1900 E Street, NW
Washington, DC 20415-0001

Patrick E. McFarland, Inspector General
Office of Personnel Management
1900 E Street, NW, Room 6400
Washington, DC 20415-1100
☎Fraud, Waste, and Abuse:
202-606-2423
☎Healthcare Fraud: 202-418-3300

Martin J. Dickman, Inspector General
Railroad Retirement Board
844 North Rush Street, Room 450
Chicago,. IL 60611-2092
☎800-772-4258

Elaine Kaplan, Special Counsel*
Office of Special Counsel
1730 M Street, NW, Suite 300
Washington, DC 20036
☎Disclosure: 800-572-2249
☎Hatch Act Information: 800-854-2824
☎Whistleblower Protection: 800-572-2249

Phyllis Fong, Inspector General
Small Business Administration
409 Third Street SW, 7th Floor
Washington, DC 20416
☎ 800-767-0385 or 202-205-7151

James G. Huse, Jr., Inspector General
Social Security Administration
Altmeyer Building, Suite 300
6401 Security Boulevard
Baltimore, MD 21235
☎800-269-0271

Jacquelyn L. Williams-Bridgers
Inspector General
Department of State and the
Broadcasting Board of Governors
2201 C Street, NW, Room 6817
Washington, DC 20520-6817
☎202-647-3320 (Collect Calls Accepted)

Kenneth M. Mead, Inspector General
Department of Transportation
400 Seventh Street, SW, Room 9210
Washington, DC 20590
☎800-424-9071 or 202-366-1461

Jeffrey Rush, Jr., Inspector General
Department of the Treasury
740 15th Street, NW,
Washington, DC 20220
☎800-359-3898

David C. Williams, Inspector General
Treasury Inspector General for
Tax Administration
1111 Constitution Ave, NW, Room 3031
Washington , DC 20224
☎800-366-4484

Richard J. Griffin, Inspector General
Department of Veterans Affairs
810 Vermont Avenue NW, Room 1114 TW
Washington, DC 20420
☎800-488-8244

*Also members of the ECIE

The Executive Council on Integrity and Efficiency Membership Addresses and Hotline Numbers

Joshua Gotbaum, Acting Chair
Executive Associate Director and Controller
Office of Management and Budget
17th and Pennsylvania Ave., NW
Room 254, Eisenhower EOB
Washington, DC 20503

Barry R. Snyder, Vice Chair, ECIE
Inspector General
Federal Reserve Board
Mail Stop 300
20th Street and Constitution Avenue, NW
Washington, DC 20551
☎800-827-3340 or 202-287-3676

Fred E. Wiederhold, Jr.
Inspector General
Amtrak
10 G Street, NE, Suite 3W-300
Washington, DC 20002-4285
☎800-468-5469

Hubert N. Sparks, Inspector General
Appalachian Regional Commission
1666 Connecticut Ave., NW, Suite 215
Washington, DC 20235
☎800-532-4611

Roy Lavik, Inspector General
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
☎202-418-5510

Mary B. Wyles, Inspector General
Consumer Product Safety Commission
4330 East West Highway
Bethesda, MD 20814-4408
☎301-504-0573

Kenneth Konz, Inspector General
Corporation for Public Broadcasting
901 E Street, NW
Washington, DC 20004-2006
☎800-599-2170 or 202-783-5408

Aletha L. Brown, Inspector General
Equal Employment Opportunity
Commission
1801 L Street, NW, Suite 3001
Washington, DC 20507
☎800-849-4230 or 202-663-7020

Eldon W. Stoehr, Inspector General
Farm Credit Administration
1501 Farm Credit Drive, Suite 4100
McLean, VA 22102-5090
☎800-437-7322 or 703-883-4316

H. Walker Feaster, III, Inspector General
Federal Communications Commission
445 12th Street, SW, Room 2-C762
Washington, DC 20554
☎202-418-0473

Lynne A. McFarland, Inspector General
Federal Election Commission
999 E Street, NW, Room 940
Washington, DC 20463
☎202-694-1015

Edward Kelley, Inspector General
Federal Housing Finance Board
1777 F Street, NW
Washington, DC 20006
☎800-276-8329 or 202-408-2900

Francine C. Eichler, Inspector General
Federal Labor Relations Authority
607 14th Street, NW, 2nd Floor
Washington, DC 20424-0001
☎800-331-3572

Tony P. Kominoth, Inspector General
Federal Maritime Commission
800 N. Capitol St., Rm. 1054
Washington, DC 20573
☎202-523-5865

Frederick J. Zirkel, Inspector General
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
☎202-326-2800

Robert G. Andary, Inspector General
Government Printing Office
N. Capitol and H Streets, NW (Stop: IG)
Washington, DC 20401
☎800-743-7574

Edouard R. Quatrevaux, Inspector General
Legal Services Corporation
750 First Street, NE, 10th Floor
Washington, DC 20002-4250
☎800-678-8868 or 202-336-8936

Paul Brachfeld, Inspector General
National Archives and Records
Administration
8601 Adelphi Road, Room 1300
College Park, MD 20740
☎800-786-2551 or 301-713-7305

H. Frank Thomas, Inspector General
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314-3428
☎800-778-4806 or 703-518-6357

Edward Johns, Inspector General
National Endowment for the Arts
1100 Pennsylvania Ave., NW, Room 528
Washington, DC 20506
☎202-682-5402

Sheldon L. Bernstein, Inspector General
Nat'l. Endowment for the Humanities
1100 Pennsylvania Ave., NW, Room 419
Washington, DC 20506
☎202-606-8423

Jane E. Altenhofen, Inspector General
National Labor Relations Board
1099 14th Street, NW, Room 9820
Washington, DC 20570
☎800-736-2983

Christine C. Boesz, Inspector General
National Science Foundation
Wilson Boulevard, Room 1135
Arlington, VA 22230
☎800-428-2189

Victor Diamond, Inspector General*
Panama Canal Commission
APO AA 34011-2300
Unit 2300
☎800-622-2625 ext. 272-7801

Charles D. Smith, Inspector General
Peace Corps
1111 20th Street, NW
Washington, DC 20526
☎800-233-5874

Wayne Robert Poll, Inspector General
Pension Benefit Guaranty
Corporation
1200 K Street, NW, Suite 470
Washington, DC 20005-4026
☎800-303-9737

Walter Stachnik, Inspector General
Securities and Exchange Commission
450 Fifth Street, NW, Stop 1107
Washington, DC 20549
☎202-942-4460

Thomas D. Blair, Inspector General
Smithsonian Institution
955 L'Enfant Plaza, SW, Room 7600
Washington, DC 20560-0905
☎292-287-3676

George T. Prosser, Inspector General
Tennessee Valley Authority
400 W. Summit Hill Drive, Room ET4C-K
Knoxville, TN 37902-1499
☎800-323-3835

Dev Jagadefan, Acting Inspector General
U.S. International Trade Commission
500 E Street, SW, Room 515
Washington, DC 20436
☎800-500-0333

Karla W. Corcoran, Inspector General
United States Postal Service
1735 N. Lynn Street
Arlington, VA 22209-2020
☎888-USPS-OIG (888-877-7644)

*The Panama Canal Commission reverted to Panama at the end of FY 1999.

GLOSSARY OF COMMON ACRONYMS AND ABBREVIATIONS

ACDA	Arms Control and Disarmament Agency
ADP	automatic data processing
AID	Agency for International Development
ARC	Appalachian Regional Commission
CIO	Chief Information Officer
CNS	Corporation for National Service
CPB	Corporation for Public Broadcasting
DCAA	Defense Contract Audit Agency
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
ECIE	Executive Council on Integrity and Efficiency
ED	Department of Education
EEOC	Equal Employment Opportunity Commission
EPA	Environmental Protection Agency
ECIE	Executive Council on Integrity and Efficiency
FBI	Federal Bureau of Investigation
FCA	Farm Credit Administration
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FEMA	Federal Emergency Management Agency
FHFB	Federal Housing Finance Board
FLRA	Federal Labor Relations Authority
FRB	Federal Reserve Board
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	General Accounting Office
GPO	Government Printing Office
GPRA	Government Performance and Results Act
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Department of Housing and Urban Development
IG	Inspector General
IGATI	Inspectors General Auditor Training Institute
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
ITC	International Trade Commission
IV&V	independent validation & verification
LSC	Legal Services Commission
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NEA	National Endowment for the Arts
NEH	National Endowment for the Humanities

NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OIRM	Office of Information Resources Management
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PBGC	Pension Benefit Guaranty Corporation
PC	Peace Corps
PCC	Panama Canal Commission
PCIE	President's Council on Integrity and Efficiency
RRB	Railroad Retirement Board
SBA	Small Business Administration
SEC	Securities and Exchange Commission
SI	Smithsonian Institution
SSA	Social Security Administration
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TVA	Tennessee Valley Authority
USDA	Department of Agriculture
USIA	U.S. Information Agency
USPS	U.S. Postal Service
VA	Department of Veterans Affairs
Y2K	Year 2000