



A Progress Report to the President



President's Council on Integrity and Efficiency
Executive Council on Integrity and Efficiency



Fiscal Year 2001 Results of OIG Efforts

The work of more than 9,600 employees of Offices of the Inspector General government-wide during FY 2001 contributed to results that include:

- Potential savings of over \$24.5 billion (includes management decisions on OIG recommendations that funds be put to better use and questioned costs)
- Recovery Actions of over \$3.7 billion
- More than 7,600 successful prosecutions
- Suspensions or debarments of nearly 9,000 individuals or businesses
- More than 2,000 civil or personnel actions
- Almost 5,000 Indictments and Criminal Informations
- More than 70 testimonies before the Congress on issues of national interest.

These accomplishments reflect the work of the 57 Offices of Inspector General, whose combined FY 2001 budgets totaled about \$ 1.4 billion.

Contents

Foreword	1
Executive Summary: Helping Federal Agencies Face New and Old Top Management Challenges	3
The Inspector General Community	9
Committee Accomplishments.....	13
Statistical Summaries of Accomplishments	18
A Compendium of OIG Activities in FY 2001.....	37
PCIE Membership Addresses and Hotline Numbers	69
ECIE Membership Addresses and Hotline Numbers	70
Acronyms and Abbreviations Glossary	71

Foreword

The members of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE) are pleased to issue this year's annual report to the President. This report highlights the exemplary accomplishments of the 57 individual Offices of Inspector General (OIG) during fiscal year (FY) 2001 and directs attention to a number of key initiatives that our organizations have addressed. This report also highlights the contributions of the dedicated OIG employees who assisted in the work related to the September 11 tragedy, an event that tried not only our resolve as a Nation, but the way the Executive Branch operates as well.

Our mission and the more than 9,600 men and women charged with putting it into effect make the Inspector General (IG) community a significant, positive force for improving the economy, efficiency, and effectiveness of Federal programs and operations and for preventing and detecting fraud, waste, abuse, and mismanagement. This report highlights the successes of the IG community in sharpening the management capabilities of our agencies, along with our findings of shortcomings and our recommendations for addressing them.

Through the thousands of independent audits, investigations, evaluations, and other activities we conducted during FY 2001, the OIGs accounted for over \$28 billion in saved and recovered Federal funds, as well as thousands of prosecutions, civil and personnel actions, and suspensions and debarments of businesses and individuals for wrongdoing. The statistical accomplishments we underscore throughout the report point to a 20-fold return on the taxpayers' \$1.4 billion investment in the OIGs.

A critical function of each OIG is to determine the most important management challenges its agency faces. As documented in this report, IGs have encountered deficiencies common to a host of agencies across the full spectrum of Government operations and programs, requiring the best collaborative efforts and attention of the IG community, administration leadership, and agency managers. Many of the challenges discussed in this report are consistent with administration initiatives detailed in the President's Management Agenda. This report also discusses a number of serious management challenges, four of which merit special emphasis. Federal agencies need to:

- ❑ Continue to address the protection of our Nation's physical and information infrastructure as part of the overall "Homeland Security" initiative.
- ❑ Improve the acquisition and management of information technology systems, and develop the capacities these systems offer for enhancing communications and performance.
- ❑ Develop appropriate program performance measures and apply them to agency budgets and management decisionmaking.
- ❑ Emphasize Government accountability and transparency by requiring Federal financial management systems to provide timely, accurate, and useful information.

This year we are prouder than ever of both the individual OIGs' accomplishments in sound management, law enforcement, and homeland security and the IG community's progress in strengthening cooperation to further these efforts. We have shared our best practices with one another, with agency management, and with the public through forums, congressional testimony, and other communication vehicles. Information on IG community initiatives and the active committees of the PCIE and ECIE is further detailed in this report and can be found on the community's Web site, IGnet (www.ignet.gov), which also contains links to our members' Web sites.

As individual IGs and as a community, we are committed to work together to carry out the mission established for us 23 years ago. We look forward to continued cooperation with the administration and Congress to address the ever-changing challenges our Government faces.



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



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

Executive Summary: Helping Federal Agencies Face New and Old Top Management Challenges

Helping to fight terrorism, evaluating the Nation's critical infrastructure, striving to improve the Government's financial management, and validating agency performance and accountability measures are among the key tasks facing the Nation's IGs today. These tasks have emerged as a result of priorities established by the administration or Congress, or, more recently, in response to threats against our homeland. These priorities are sharply different from the ones the newly designated IGs faced 23 years ago.

In 1978, the IG Act was signed, creating 12 independent audit and investigative offices. At that time, the IGs were charged with independently reviewing the programs and operations of their agencies; detecting and preventing fraud, waste, and abuse; and promoting economy, efficiency, and effectiveness so their agencies could best serve the public. While the act has since been amended several times to add new IGs and clarify reporting requirements, these basic tenets have remained constant and strong. Today, 57 OIGs provide oversight to 59 Federal agencies.

Individual OIGs view themselves as "agents of positive change" within their agencies and direct their work toward examining programs and operations to promote program efficiency and effectiveness and protect Government integrity. IGs strive to be influential forces by identifying vulnerabilities in their agency's programs and operations and by facilitating excellence by recommending improvements. While changes in vulnerability and risk have affected the focus of their work and priorities over the years, the OIGs have drawn on their broad base of knowledge and expertise to adapt to these changes and remain relevant and on point.

Our report this year continues to demonstrate the tangible savings and contributions to a sound Federal Government that the OIG community of over 9,600 employees has identified through its various audits, evaluations, inspections, investigations, and other activities. Overall, Federal departments and agencies agreed to savings or recoveries totaling over \$28 billion in Federal monies that OIGs identified. Other OIG actions resulted in more than 7,600 successful prosecutions, almost 5,000 indictments and criminal informations, and more than 2,000 civil or personnel actions against individuals or entities. Also, the OIGs reported suspensions or debarments of nearly 8,800 contractors, grantees, and other entities or individuals doing business with the Government. OIGs testified more than 70 times before congressional committees on a broad range of matters of national interest. Of course, these figures do not include the intensive efforts of the many dedicated OIG employees who assisted in the work related to the September 11 tragedy.

Clearly, the OIGs bring longstanding historical perspectives, stability, and integrity to bear on the challenges, opportunities, and difficult times facing our Government. As evidenced in this report, the IG community continues to demonstrate its dedication to its homeland, commitment to good government through its management challenges work and support of the President's Management Agenda, and obligation to its basic mission. An overview of these issues follows, with specifics beginning on page 37 of this report.

IG Community's Response to the September 11 Terrorist Attacks

September 11, 2001, is a day that Americans will never forget. The deaths of more than 3,000 people at the hands of a well-orchestrated terrorist attack will remain etched in our minds and hearts. While the realization that these attacks could and did take place on American soil was all too frightening, a renewed sense of patriotism, cooperative spirit, and faith in the American dream emerged throughout the Nation. The IG community felt this same determination and mobilized itself to help restore the calm, collect and analyze evidence, and support initiatives to combat terrorism.

Immediately following the attacks, hundreds of OIG special agents and other personnel participated in rescue and evidence recovery efforts at the World Trade Center, the Pentagon, and the Pennsylvania crash site. That day, OIG special agents helped the New York/New Jersey Port Authority transport more than 160,000 people from New York City across the river to New Jersey, while other agents from the IG community assisted in initial search and rescue efforts at the Pentagon. Twenty-one OIGs sent teams of special agents to the Pentagon and World Trade Center to assist in evidence recovery, working 12-hour shifts to find airplane parts and identify victims.

In the aftermath of these disastrous attacks, the IG community responded quickly and in large numbers to provide strong and widespread support to the efforts to answer such questions as where the terrorists came from, how they concealed themselves in our society, how they financed their operations, and what support they had within the United States. Almost every IG provided the Federal Bureau of Investigation (FBI) and other law enforcement agencies with investigative assistance and resources to identify, interview, and arrest suspects. They also helped trace funds; conducted record checks, searches, and surveillance; and provided computer forensic support. OIG agents with specific expertise also contributed significantly to the FBI's anthrax and bioterrorism investigation by helping to identify potential suspects and assisting in screening and investigating suspicious mail.

Since the attacks, the support of the IG community has not wavered. OIGs are continuing to support various initiatives to secure our homeland. For example, OIGs from around the country have contributed to safeguarding our Nation's airways by detailing special agents from the Federal law enforcement community to the Federal Air Marshal program. In addition, OIGs have refocused their audit work not only to examine the systemic vulnerabilities that failed to prevent or detect the crimes--or even facilitated their occurrence--but also to explore other homeland vulnerabilities that could be future targets of terrorism.

Top Management Challenges Highlight Security and Good Government

Throughout 2001, the members of the PCIE and ECIE continued to bring to bear their collective perspective, expertise, and resources to confront the Federal Government's top challenges more effectively and efficiently. Individually, IGs across the Government identified the management challenges posing the greatest risk to programs and operations at their respective agencies. Clearly, the security of our Nation's physical and information infrastructure tops the list of challenges facing many agencies. Good government issues—such as information technology management and financial management reform—continue to rank high as significant challenges. These are real issues, requiring the sustained attention of Congress, the administration, Federal managers and employees, and the IG community.

Although the IG community can assist agencies and Congress in identifying and addressing these challenges, support from the administration and the public is critical. In August 2001, the administration announced the President's Management Agenda, which targets five Governmentwide reform initiatives—human capital management, competitive sourcing, financial performance improvement, expanded electronic government, and budget and performance integration—as its immediate focus for achieving a more responsible and responsive Government that is citizen-centered, results-oriented, and market-based. Each of these five initiatives closely correlates with areas that the OIGs have designated as top management challenges. As in years past, the PCIE and ECIE have once again compiled these challenges into a short report to the Chairman and Ranking Member of the House Committee on Government Reform, to focus attention on areas that warrant high-level attention and review.

While vulnerability and risk changed dramatically during 2001, the IGs remained vigilant in addressing top management challenges and positioning their organizations to further advance agency progress in these critical initiatives, as highlighted below.

Protecting the Nation's Physical and Information Infrastructures— "Homeland Security"

Historically, many of the Nation's critical infrastructures have been physically and logically separate systems with little interdependence. Advances in information technology (IT), however, have created new vulnerabilities to terrorism, equipment failures, human error, weather and other natural causes, and cyber-attacks. Securing the Nation's critical infrastructure is essential to economic and national security, and homeland security has become a priority of the administration. All IGs recognize physical and information infrastructure as a top management challenge.

IGs are also conducting annual independent evaluations of their agencies' information security programs and practices as part of the Government Information Security Reform Act (GISRA), which codifies and reiterates existing security policies and responsibilities. The PCIE and ECIE are continuing to collaborate on a four-phase review of Federal agencies' implementation of Presidential Decision Directive (PDD) 63, which calls for a national effort to ensure the security of critical infrastructures. During 2001, the OIGs reported on opportunities to improve the Government's planning and assessment activities for critical cyber-based infrastructure assets. Individually, OIGs have accelerated a review of controls over accidental or intentional release of biohazards, emphasizing pathogen accountability and personnel and physical security at key Federal laboratories.

Managing Information Technology and the Transition to Electronic Government

In an increasingly interconnected society, Americans use the telephone and the Internet to obtain services 24 hours a day, 7 days a week. More than 60 percent of all Internet users interact with more than 31 million Federal Web pages on 22,000 Government Web sites, and this number is growing. The President's Management Agenda cites expanded electronic government (E-Government) as a key Governmentwide initiative aimed at:

- ❑ Making it easy for citizens to obtain services and interact with the Federal Government.
- ❑ Improving Government's efficiency and effectiveness.
- ❑ Improving Government's responsiveness to citizens.

OIGs across the Federal Government agree that electronic technology can be used efficiently and effectively to improve services to the American taxpayer. They have begun reviewing E-Government initiatives with a view to ensuring that appropriate controls are in place to safeguard the sensitive data and critical systems of Government. Under the Government Paperwork Elimination Act (GPEA), executive agencies must move to E-Government by October, 2003. The purpose of GPEA is not simply to replace paper transactions with electronic ones, but to help agencies improve operations, achieve cost savings, and develop adequate controls to prevent fraud, waste, and abuse. With the Federal Government expecting to spend more than \$50 billion in 2003 on E-Government issues, the IG community plays a vital role in overseeing the management of information technology and the resources dedicated to E-Government.

The OIGs also recognize that the growth of Web access and E-Government, the availability of electronic access under the Freedom of Information Act (as amended by the Electronic Freedom of Information Act), and the implementation of GPEA will further increase demands for online records and services. IG work during 2001 pointed out the importance of mastering the challenges of preserving electronic records in a way that makes them available in systems through which users can locate, retrieve, and read them.

Better Integration of Budget and Performance Results

The administration's focus on improving program results while controlling costs is emphasized through its integration of budget and performance initiatives. Although Federal departments and agencies have developed plans and reported on their performance as required by the Government Performance and Results Act (GPRA), this information has not been aligned or included in their budget submissions to the Office of Management and Budget (OMB). The U.S. General Accounting Office (GAO) also has reported that additional effort is needed to describe clearly the relationship among performance expectations, requested funding, and consumed resources.

The IG community continues to consider GPRA implementation and accountability as significant agency challenges. Last year, we responded to Chairman Dan Burton of the House Government Reform Committee on the OIGs' assessment of the most significant performance measures contained in their respective agencies' performance reports and the extent to which the data or information underlying the measures was valid and accurate.

Many of the OIGs have made the assessment of GPRA-related performance measures a standard part of their work and have identified areas for improving performance budgeting, streamlining time-tracking systems, simplifying tracking of product and service costs, and implementing other enhancements to the performance management framework. Agencies also will need to upgrade their financial and program information systems to generate the appropriate information for fully integrating their budget and performance programs.

Improving Financial Performance

With improved financial performance prominently featured in the President's Management Agenda, the administration is aggressively seeking to improve the timeliness, usefulness, and reliability of financial information to enable sound decisionmaking and safeguard the Government's assets. Since the enactment of key legislation during the 1990s to improve Federal financial management, OIGs also have worked closely with Federal entities to address financial management and accounting system weaknesses. As a result of this concerted effort, 18 of 24 Chief Financial Officer (CFO) Act agencies received unqualified or "clean" opinions on their FY 2001 financial statements.

Much more needs to be done to improve the quality, timeliness, and usefulness of financial information and enhance financial information systems. Our experience shows, however, that for some agencies, attainment of a clean opinion is a fragile and somewhat artificial achievement because it results from extraordinary end-of-year efforts rather than a more constant real time financial management system operation. The administration's emphasis on accelerating the reporting requirements over the next few years, to require in 2004 an audited financial statement within 45 days after the end of the FY, will challenge the community. The CFO and IG communities are working together to address this emerging issue.

Agencies will need to further streamline their processes and/or upgrade their financial information systems to achieve this goal. In June 2001, the IG community issued its "Best Practices Guide: Coordinating the Preparation and Audit of Federal Financial Statements" to share methods OIGs use to coordinate the financial statement audits within their agencies. Together with GAO, we have revised the "Financial Audit Manual," which provides auditors with a single reference for auditing agency financial statements. The IG community and CFOs are also conducting a joint project to determine the extent of erroneous payments and identify ways to address this \$20 billion problem.

Addressing the Strategic Management of Human Capital

The wave of expected retirements, recruitment and retention obstacles, inadequate evaluation and reward systems, and outdated training and education methods are areas that need immediate

attention. GAO has announced that these areas present a “high-risk” factor for the Federal Government’s ability to sustain its continued level of services to the public. According to GAO, more than half the Federal workforce, or about 900,000 employees, will be eligible to retire by 2005. The administration is addressing this risk by asking each agency to develop a viable human resource strategy to attract and retain the right people, in the right places, and at the right time. This strategy should enable each agency to be a high-performance organization that delivers high-quality services to the American public.

Members of the IG community agree that human capital management is a major challenge, not only for their respective agencies but also for their own organizations. Many OIGs have reported that agencies could address their human capital issues through workforce skills and competency assessments, benchmarking against other Federal or private sector organizations, succession planning, innovative recruitment and hiring approaches, improved training opportunities and techniques, adoption of appropriate workplace tools, and other workforce planning strategies. The PCIE also has aligned its committee structure by establishing a Human Resource Committee to create and implement innovative and effective human resource management programs within the community.

Managing Procurement and Competitive Sourcing

With the dual goals of improving performance and cutting costs, the President’s Management Agenda places increased emphasis on creating competition between Federal and private sources for certain tasks that are readily available in the commercial marketplace, such as administrative support, certain aspects of facilities management, and payroll services. Under the Federal Activities Inventory Reform (FAIR) Act, agencies and the OIGs are identifying functions that could be performed by the private sector. With this emphasis on “market-based” government, the OIGs’ independent assessment of agency contracting activities takes on added importance.

As a note of caution, we must point out that the Federal Government has been lax in its contractor oversight. Our annual reports to the President—including the compendium in this report—are full of examples of poor contractor oversight resulting in excessive and unnecessary costs. Even more alarming, fraudulent billing schemes can result. OIG investigative work continues to confirm the vulnerability of programs to general contract fraud and embezzlement, and has resulted in the recovery of billions of dollars. Appropriate internal controls and effective oversight must be in place to ensure that the goods or services are not only meeting the needs of the Government and the public but are provided in the most cost-effective and efficient manner. The OIGs continue to identify procurement and grant management as a major management challenge.

Conclusion

Across Government, IGs face expanding challenges as we work with agencies to address the myriad issues confronting the Federal Government. We contribute to a comprehensive national strategy to secure the United States from terrorist threats or attacks. We have taken the lead in evaluating threats to physical and information infrastructure since September 11, 2001, and in making detailed recommendations for addressing them. Homeland security has become one of the top management challenges our agencies face.

OIGs also add value by their constant focus on improving Government operations and enhancing service to the public—successfully using their authority to be independent voices for Federal economy, efficiency, and effectiveness. Many of our top management challenges mirror the President’s Management Agenda of Government reform initiatives, such as expanding electronic government and improving financial performance. We play a dynamic role in focusing the attention of Congress, the administration, and Federal managers and employees on problems and solutions.

Collectively, the PCIE and ECIE continue to help to improve Government programs and operations. We are working in greater collaboration than ever before with agency managers to present audits and recommendations that are fair, constructive, and reasonable. In addition, our investigations help narrow the opportunities for misconduct and corruption within the Federal Government and among citizens and businesses the Federal Government serves. Our goal is for every criminal and administrative investigation to produce systemic and procedural reforms to prevent future abuse.

Both as individual IGs and as a community, we look forward to building on our cooperative working relationships with Congress, the administration, and Federal managers, so that together we can continue to make substantive progress in resolving the top management challenges facing the Federal Government.

The Inspector General Community

In October 1978, Congress passed and the President signed the IG Act, 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 these auditors and investigators were frequently part of the programs they were reviewing. This splintered system made it hard for these small audit and investigative offices to see patterns of abuse in their agencies' programs.

The 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 because of the recommendations from IG reports. As a result of this success, the IG concept has been gradually expanded to most of the Federal Government. In FY 2001, 57 OIGs were providing oversight to 59 Federal agencies.

The modern civilian IG was derived from the military custom of having an IG 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

IGs are different from other Federal officials because of their independence. This statutory independence is intended to ensure the impartiality of their audits and investigations. IGs report both to the heads of their respective agencies and to Congress. This dual reporting responsibility is the framework within which IGs perform their functions. It is the legislative safety net that protects IG independence and objectivity.

Specifically, the IG Act authorizes IGs to do the following:

- ❑ Conduct audits and investigations and issue reports as they believe appropriate (with limited national security, financial market, 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 the agency head.
- ❑ Administer oaths for taking testimony.
- ❑ Hire and control their own staff and contract resources.
- ❑ Request assistance from any Federal, State, or local government.

IGs often seek input from stakeholders on what projects and areas 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 Congress. Many IGs also participate in their agencies' senior councils, and OIG staff frequently provide advice on management policies as they are developed.

Mission

In simple terms, IGs have two basic roles—to find and report on current problems and to foster good program management to prevent future problems. This annual report discusses how IGs meet their specific statutory mission by:

- ❑ Conducting and supervising audits, investigations, and inspections relating to the programs and operations of their agencies.
- ❑ Reviewing existing and proposed legislation and regulations relating to the programs and operations of their agencies.
- ❑ Providing leadership for activities designed to promote economy, effectiveness, and efficiency, and promote efforts to reduce fraud, waste, and abuse in their agencies' programs.
- ❑ Informing their agency heads and Congress of problems in their agencies' programs and operations and of the need for and progress of corrective actions.

In performing this mission, OIGs prepare a variety of reports. During FY 2001, OIGs collectively issued more than 4,100 reports and provided some 70 testimonies before congressional committees. In addition, OIGs closed more than 29,700 investigations and processed nearly 228,800 complaints. The reports include the following:

Audit Reports. The IG Act requires OIG audits to be performed under auditing standards established by GAO. OIG audits evaluate:

- ❑ Performance of agency programs and supporting administrative and financial systems.
- ❑ Compliance with relevant laws and regulations.
- ❑ Ways funds could be put to better use.
- ❑ Fulfillment of responsibilities to the Government by contractors and/or grantees.
- ❑ Entitlement of individuals or firms doing business with or receiving benefits from the Government to have received funds and whether they should make restitution.

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

Inspection Reports. Inspections include policy and program evaluations. Several OIGs have adopted inspections as a quick way to spot-test the effectiveness of agency programs or to do a broad review on issues that affect agency programs. The PCIE and ECIE have adopted professional standards to promote the validity and independence of OIG inspections.

Investigation Reports. In accordance with professional guidelines established by the PCIE and ECIE and, in certain cases, guidance from the Department of Justice (DOJ), OIGs investigate both criminal and administrative wrongdoing against agency programs and operations. IGs are empowered to investigate anyone who may have defrauded their agencies' programs. They may investigate beneficiaries, contractors or grantees, or Federal officials. IGs are required to report suspected violations of criminal law directly to the Attorney General and frequently work cooperatively with the DOJ's United States Attorneys on criminal investigations.

Semiannual Reports to Congress. These reports, specifically mandated by the IG Act, require IGs to summarize their most significant recent reports and management's action on significant IG recommendations. The reports provide a useful overview of OIG activity and demonstrate the contributions of each IG.

IG Appointments

IGs are selected on the basis of their personal integrity and expertise in accounting, auditing, financial analysis, law, management analysis, public administration, or investigations. The IGs serving in Cabinet-level departments and sub-Cabinet agencies are nominated by the President and confirmed by the Senate. These IGs can be removed only by the President, who must communicate the reasons for any such removal to both houses of Congress.

IGs at certain independent agencies, corporations, and other Federal entities—called “designated Federal entities”—are appointed by the heads of those entities, who may also remove the IGs from office. If they are removed, the entity head must notify both Houses of Congress of the reasons for removal.

President's Council on Integrity and Efficiency

The presidentially-appointed IGs work together and coordinate their professional activities through the PCIE. This Council, which was created by Executive Order 12301, Integrity and Efficiency in Federal Programs, dated March 26, 1981, and updated in 1986 by Executive Order 12625 and in 1992 by Executive Order 12805, works to promote collaboration on integrity, economy, and efficiency issues that transcend individual Government agencies and to increase the professionalism and effectiveness of OIG personnel throughout the Government.

The Deputy Director for Management of OMB chairs the PCIE and is responsible for reporting to the President on its activities. In addition to the presidentially-appointed IGs, members include the Controller of OMB's Office of Federal Financial Management, the Special Counsel from the Office of Special Counsel (OSC), the Director of the Office of Government Ethics (OGE), the Deputy Director of the Office of Personnel Management (OPM), and the Assistant Director, Criminal Investigative Division, FBI. The Vice Chair, who is recommended by the PCIE members and approved by the Chair, manages the Council's day-to-day activities. The Vice Chair is also a member of the ECIE.

Executive Council on Integrity and Efficiency

IGs of designated Federal entities work together and coordinate their professional activities through the ECIE. This Council, also created by Executive Order 12805 on May 11, 1992, has the same mission as the PCIE—to address integrity and efficiency issues that transcend individual Government agencies and to increase professionalism and effectiveness of OIG personnel throughout the Government. OMB's Deputy Director for Management also chairs the ECIE. In addition to the IGs, the ECIE includes the Controller of OMB's Office of Federal Financial Management, the Special Counsel of OSC, the Director of OGE, the Deputy Director of OPM, and the Assistant Director, Criminal Investigative Division, FBI. The Vice Chair, who is recommended by the ECIE members and approved by the Chair, manages the Council's day-to-day activities. The Vice Chair is also a member of the PCIE. The ECIE also has representatives on PCIE committees.

PCIE and ECIE Activities

The PCIE and the ECIE rely on the Vice Chair offices and the PCIE standing committees to oversee their many activities. Members of both Councils joined together in roundtables and working groups throughout the year to address a wide range of relevant issues, including auditing standards, information technology security, and misconduct in research. The work of the six standing committees is summarized in the next section of this report.

In May 2001, both Councils adopted a strategic framework that laid out their mission, vision, goals, objectives, and strategies for the next 3 years. This framework sets out a strategy for members of both Councils to fulfill their agency missions as well as collectively contributing to resolving

Governmentwide challenges. In the fall of 2001, the Councils published "A Strategic Framework" and prepared a companion brochure on the IG community to share with stakeholders.

Also in May 2001, the PCIE and ECIE held their annual conference, entitled *Managing in a Time of Change*. The conference gave the members an opportunity to hear from Congress, the administration, and Federal managers on the critical challenges facing the Government and the opportunities for the IG community to add value.

During its annual awards program held in the fall, the community recognized more than 450 individuals for outstanding performance and commitment to fulfilling the IG mission. During this program, the community recognized June Gibbs Brown, former IG at the Department of Health and Human Services (HHS), as the first recipient of the June Gibbs Brown Career Achievement Award. After receiving her award, Ms. Brown assisted in presenting five additional career achievement awards bearing her name.

In addition, the Councils publish the *Journal of Public Inquiry* twice a year. The *Journal* consists of a compilation of articles by members of the IG community, scholars, professionals outside the Federal Government, and others on topics important to the IG community. In FY 2001, three editions were published, focusing on the important challenges facing the new administration, human capital issues, information technology, and other issues germane to the IG community. All *Journal* editions can be found on the IG Web site at www.ignet.gov/randp/jpi.

Finally, the PCIE maintains two training centers for OIG staff: the Inspectors General Auditor Training Institute (IGATI) at Fort Belvoir, Virginia, and the Inspector General Criminal Investigator Academy (Academy) at the Federal Law Enforcement Training Center in Glynco, Georgia.

More information on PCIE, ECIE, and individual OIG activities is available on IGnet at www.ignet.gov.

Committee Accomplishments

PCIE, in conjunction with ECIE, maintains six standing committees and other groups to examine important issues and assist the Councils in their ongoing efforts to promote integrity, accountability, and excellence in Government. Below is a discussion of each committee's accomplishments for FY 2001.

Audit Committee

Inspector General Gregory H. Friedman of the Department of Energy (DOE) chairs the Audit Committee. During FY 2001, the Audit Committee continued to provide leadership in matters within its purview, including providing oversight to IGATI, which trained more than 1,700 auditors during the year.

The committee continued its efforts to promote relevant, high-profile, crosscutting initiatives by multiple OIGs in areas of interest to Congress, the administration, and others. In FY 2001, the committee helped facilitate efforts of the Social Security Administration (SSA) OIG to lead a multiagency review of controls over Social Security numbers (SSN). It is anticipated that the results of this review will have significant implications both within individual Government agencies and with respect to larger national concerns over homeland security, identity theft, and related challenges.

In March 2001, the committee issued "Review of Federal Agencies' Implementation of Presidential Decision Directive 63 Related to Critical Infrastructure Protection." Critical infrastructures are the physical and cyber-based systems essential to the minimum operations of the economy and Government. They include banking and finance, telecommunications, energy, transportation, and essential Government services. These matters took on even more significance in the aftermath of September 11. The report can be found at www.ignet.gov/pande/audit/dreport.pdf.

The committee published the "Financial Audit Manual" (FAM), a joint effort of PCIE and GAO. The issuance of this document marks the first time that the PCIE community and GAO will have a single reference for auditing agency financial statements. The two volumes of the FAM can be found at www.ignet.gov/pande/audit/famvol1.pdf and www.ignet.gov/pande/audit/famvol2.pdf.

In addition, the committee formed an interagency team tasked with updating the "Audit Peer Review Guide," helping to ensure that OIG audit operations comply with current and emerging standards for audit integrity and professionalism. The committee also contributed to the improvement of the overall quality of single audit efforts, in part by helping to update the "Federal Cognizant Agency Audit Organization Guidelines."

Finally, the committee released "Best Practices Guide for Financial Statement Preparation and Audit Activities," a compendium of best practices from Federal OIGs and CFOs. This guide can be found at www.ignet.gov/pande/audit/affs0601.pdf.

Human Resources Committee

Nikki Tinsley, the Environmental Protection Agency (EPA) IG, chairs the Human Resources Committee. During FY 2001, the Professional Development Committee initiated plans for a new direction to focus its efforts and was renamed the Human Resources Committee. Discussions were held to identify the best methods to serve the IG community and to address the strategies set forth in the PCIE and ECIE Strategic Framework.

Suggestions included creating a centralized clearinghouse for training information, cross-training auditors and investigators, establishing partnerships with training institutes and universities, and developing new methods for the recruitment and retention of personnel.

The committee also organized and sponsored two forums during the year. The first forum was presented by Roger Viadero, formerly the IG of the Department of Agriculture (USDA). He addressed the importance of employee motivation by managers. Mr. Viadero shared his many audit experiences and successes at the FBI and USDA through the effective delegation of projects to staff members and the achievement of positive results.

The second forum was presented by Virginia L. Thomas, Director, Executive Branch Relations, from the Heritage Foundation. Ms. Thomas, who is responsible for helping the foundation convey its resources and ideas to the decisionmakers in the Bush administration, shared her ideas on the administration's position on issues. She also emphasized the importance of all IGs developing relationships with Members of Congress. She urged IGs to become more public about their activities and achievements.

Inspection and Evaluation Committee

Michael Mangano, Principal Deputy IG at HHS, provided interim leadership for the Inspection and Evaluation Committee after the January 2002 retirement of June Gibbs Brown.

During FY 2001, the committee pursued a number of new directions to improve the usefulness of inspections and evaluations (I&E) in supporting the work of the IG community and to share information about current issues and best practices. The committee also continued to work closely with the I&E Roundtable—the organization of assistant IGs and others who have responsibility for conducting evaluations and inspections in their respective agencies. Together, the committee and roundtable continued their efforts to further enhance I&E activity throughout the Government.

During FY 2001, the committee issued "Advisory and Assistance Services: A Practical Reference Guide." This guide for helping the IG community obtain advisory and assistance services targets OIG project officers, providing an overview of the legal and practical aspects of contracting for various "intellectual" or consulting services, as well as helpful advice for those considering the use of other service contracts. It focuses on acquisition planning, selection of contractors, and contract management and administration. The guide is available at www.ignet.gov/randp/rpts.html.

In addition, the I&E Committee continued its work in the area of child support enforcement. This multiphase project was prompted by Executive Order 12953, which mandates that the Federal Government set an example of leadership in collecting child support payments due from its employees. The committee has examined compliance with child support laws among employees of the FBI and HHS, as well as those agencies' efforts to ensure compliance. DOJ OIG issued a report on the findings of its FBI review, and HHS OIG issued a report on its findings at HHS.

The I&E Committee also provided outreach to private sector groups and other public organizations. As a result of this outreach, the committee has worked to improve the use and quality of evaluations via presentations made to the American Evaluation Association, the Eastern Evaluation Research Society, and other professional organizations, as well as new IGs.

And finally, the committee and roundtable placed vigorous emphasis on training. Together, they sponsored numerous programs to enhance the skills of evaluators and inspectors, and thus the quality of their reports. More than 120 OIG staff members from numerous agencies took advantage of the courses, which covered such topics as effective writing, statistics, questionnaire design and survey techniques, and evaluation skills and analysis.

The I&E Committee and roundtable are continuing close discussions with their membership and with the larger IG community to share findings on crosscutting issues such as bioterrorism, information security, and travel and purchase card usage; to select new roundtable projects; and to identify effective evaluation and inspection practices.

Investigations Committee

Patrick E. McFarland, OPM's IG, chairs the Investigations Committee. The purpose of the committee is to advise the Federal OIG community on issues involving criminal investigations, criminal investigative personnel, training, and the establishment of criminal investigative guidelines. In addition, the committee serves as the board of directors of the Academy, with the accountable IG from the Treasury Inspector General for Tax Administration (TIGTA). The committee relies on the Investigations Advisory Subcommittee, composed of assistant IGs for investigations, to assist in these efforts.

In FY 2001, the committee, with the assistance of the Investigations Advisory Subcommittee, addressed the following initiatives:

"Qualitative Assessment Review Guide"—A draft of the guide that outlines external peer review standards was distributed to the IG community in July 2001. As a pilot, each OIG has been asked to conduct an internal review of its investigation program, based on the draft guide. The purpose of this pilot review is for OIGs to refine the draft by commenting on the length of time it took to complete the review, any difficulties encountered as a result of the directions in the draft guide, and any other information that may be helpful in modifying the guide before final adoption.

Permanent Statutory Law Enforcement Authority—In FY 2000, Senator Fred Thompson introduced legislation (S. 3144) to confer permanent law enforcement authority on 23 presidentially-appointed and Senate-confirmed IGs. Although the bill was reported out by the Senate Governmental Affairs Committee on October 3, 2000, the Senate took no action. Efforts were continued during FY 2001 to seek support for such a permanent law enforcement authority.

IG Criminal Investigator Academy—Early in FY 2001, the President signed legislation that established the Academy, in addition to an IG Forensic Science Laboratory, under the Department of the Treasury. However, funding for the Academy and the IG Forensic Science Lab was not included in the FY 2002 or FY 2003 President's Budget Request.

Integrity Committee

Grant D. Ashley, Assistant Director of the FBI's Criminal Investigative Division, chairs the Integrity Committee. As created by the PCIE and ECIE Chair and formally established by Executive Order 12993, Administrative Allegations Against Inspectors General, the Integrity Committee receives, reviews, and refers for investigation, where appropriate, allegations of wrongdoing by IGs and, in limited cases, OIG staff. The membership of this committee, which includes representatives from the FBI, OSC, OGE, and at least three IGs appointed by the PCIE and ECIE Chair, is dictated by the Executive Order.

During FY 2001, the committee successfully managed its responsibilities, as evidenced by the statistics below. At the close of FY 2001, the committee had eight pending cases and one active investigation. The committee's accomplishments are as follows:

- ❑ Reviewed 24 new complaints.
- ❑ Processed and brought to closure 33 separate complaint matters, which included cases opened in previous years.
- ❑ Determined that 23 of the 33 complaints were outside the committee's purview and referred them to other agencies for consideration. Nine cases were unsubstantiated, and one case was closed administratively.

- ❑ Supervised two investigations into allegations of misconduct by OIG personnel. One investigation was closed owing to the complainant's refusal to cooperate in the investigation. The other was ongoing at the end of the FY.

Legislation Committee

Department of Transportation (DOT) IG Kenneth Mead chairs the Legislation Committee. The committee alerts and informs the PCIE and ECIE about legislative initiatives of interest to the IG community, particularly bills and amendments that would affect IG statutory authority or create new IG responsibilities. The committee also provides information to the entire IG community about applicable Federal statutes, concerns of particular Members of Congress, and congressional hearings of importance to IGs and their staff.

The Legislation Committee also brings together IGs and influential Members of Congress to discuss areas of mutual legislative interest. When the administration or Congress requests comments from the PCIE and ECIE on legislation or policy, the Legislation Committee serves as a central coordinating point. The committee also systematically informs all IGs, deputy IGs, IG legislative liaisons, and counsels to the IGs about legislative developments in Congress.

In FY 2001, the committee sent out more than 20 legislative alerts, advising the IG community about proposed legislation in the following areas:

- ❑ Financial management.
- ❑ Computer privacy and security.
- ❑ Law enforcement.
- ❑ Government management and operations.
- ❑ Energy management policy.

The committee also provided extensive input during development of the original fraud recovery audit legislation, which became law this year as part of the FY 2002 Department of Defense (DOD) Authorization Act (P.L. 107-107). This law requires agencies with contracting authority in excess of \$500 million to perform recovery audits to identify any overpayments to vendors providing goods and services to the Government. Sponsors of this legislation (H.R. 2547) in the House of Representatives retained provisions sought by the Legislation Committee regarding IG authority and oversight responsibilities, fraud detection and reporting, and collection of recovered funds.

Other Committees, Roundtables, and Working Groups

GPRA Coordination Committee—The mission of the GPRA Coordination Committee is to foster and advance the implementation of management performance and accountability by serving the IG community as catalysts, facilitators, and educators. This committee helped promote greater understanding and integration of the sound business practices inherent in GPRA precepts and guidelines and served as a focal point to advance knowledge and expertise within and outside the IG community. During FY 2001, under the leadership of the Department of State (DOS) OIG, the committee met with representatives from OMB, Congress, GAO, and several "good government" organizations to elicit their views on GPRA and agency progress in implementing effective planning and performance measurement. The committee established itself as a point of contact with congressional staff members interested in GPRA and assisted OIGs in responding to a request from Chairman Dan Burton of the House Committee on Government Reform. Twenty-six OIGs responded to Chairman Burton's request for the OIGs to assess the most significant performance measures contained in their agencies' performance reports and the extent to which the data or information underlying the measures was valid and accurate. Under the auspices of TIGTA OIG, the committee enhanced its Web site by providing more extensive and accessible GPRA information and resources

for the IG community, including a database of IG community performance measures that was developed by EPA OIG.

Information Technology Roundtable—The IT Roundtable, led by the National Aeronautics and Space Administration (NASA) OIG, serves as a forum for sharing IT information and best practices among members of the IG community. The IT Roundtable plays a coordinating role in developing OIG responses to national-level IT priorities and disseminating information about, and responding to, hostile activities against the national information infrastructure. In FY 2001, the NASA OIG sponsored two Governmentwide conferences, which provided both the IG and the chief information officer (CIO) communities with viewpoints from OMB, the National Institute of Standards and Technology (NIST), GAO, and law enforcement agencies regarding OIGs' GISRA responsibilities. Also, the IG community conducted reviews of PDD-63, the Presidential Decision Directive on Critical Infrastructure Protection. Twenty-one OIGs participated in the first phase of this review, which focused on agency planning and assessment activities for protecting critical cyber-based infrastructures. On March 21, 2001, the PCIE and ECIE Vice Chairs issued the Phase I report to the Director, OMB, and the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The third phase of the review also began during FY 2001.

Misconduct in Research Working Group—Sponsored by the National Science Foundation (NSF) OIG, the Misconduct in Research (MIR) Working Group was formed to educate the IG community about MIR issues and develop a set of standards for the conduct or oversight of MIR investigations. Representatives from more than 20 OIGs participated in this year's efforts. The group worked closely with the Office of Science and Technology Policy (OSTP) to host a February 2001 workshop focused on implementing the OSTP Research Misconduct Policy. More than 70 people attended this workshop, which served as a springboard for agency and OIG representatives to discuss implementation of OSTP policy within their respective agencies. Representatives of the MIR Working Group coordinated closely with the Academy to incorporate MIR materials into training modules. The group also developed a supplement to the PCIE/ECIE "Quality Standards for Investigations," which is being used to assist OIG special agents with misconduct investigations and help OIGs establish standards for conducting oversight reviews of agency investigations.

Statistical Summaries of Accomplishments

The tables on the following pages demonstrate the impact of OIGs in their agencies and summarize key accomplishments for FY 2001. The statistics included in this report are based on submissions from the reporting OIGs. The data reported are defined in most instances by the provisions of the IG Act, 5 U.S.C. app. § 5, whereby Congress established uniform reporting categories for each IG's semiannual report to Congress. Because of data limitations or features peculiar to individual OIGs, however, some variations occur, as explained in the accompanying footnotes. In addition, OIGs often participate in multiagency task forces or join with other OIGs to accomplish a common objective.

In reporting this year's investigative statistics, the IG community undertook a project to eliminate the potential for duplicative reporting of joint casework among OIGs. Traditionally, the investigative statistics have been compiled by listing the statistics reported by each OIG and then aggregating the figures for the IG community. Recognizing that this process had the potential for duplicative reporting of casework that involved multiple OIGs, the IG community conducted a study that defined consistent criteria for compiling the investigative data. Despite a few technical issues encountered during the project (which have been footnoted in the following tables), we are pleased to report that nearly all the joint efforts were identified and have been reported separately in the investigative tables. We will continue to improve on this approach for compiling investigative data in future reports.

The goal of this investigative project was to eliminate the possible duplicate reporting of statistics among the OIGs. As in the past, these statistics do include the efforts of the OIGs when their investigations are conducted jointly with traditional law enforcement agencies such as the FBI, U.S. Secret Service, U.S. Postal Inspection Service, or State and local law enforcement agencies.

Performance Profile 2001	
Summary of Combined Accomplishments of PCIE and ECIE Members	
Recommendations That Funds Be Put to Better Use	\$89,226,582,927
Management Decisions on Recommendations That Funds Be Put to Better Use	\$22,178,783,933
Questioned Costs	\$4,125,882,715
Management Decisions on Questioned Costs	\$2,341,932,048
Investigative Recoveries	\$3,748,150,897
Successful Criminal Prosecutions	7,609
Civil Actions	905
Suspensions/Debarments	8,828
Personnel Actions	1,213
Indictments and Criminal Informations	4,980

Recommendations That Funds Be Put to Better Use (Tables I-P and I-E)

The IG Act defines a recommendation that funds be put to better use as "a recommendation by the Office that funds could be used more efficiently if management of an establishment took actions to implement and complete the recommendation, including (1) reductions in outlays; (2) de-obligations of funds from programs or operations; (3) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; (4) costs not incurred by implementing recommended improvements related to the operations of the establishment, a contractor, or

grantee; (5) avoidance of unnecessary expenditures noted in pre-award reviews of contractor grant agreements; or (6) any other savings which are specifically identified."

For FY 2001, including Defense Contract Audit Agency (DCAA) audits performed in agreement with OIGs or agencies, PCIE member agencies recommended that approximately \$89.2 billion be put to better use; ECIE member agencies recommended that approximately \$67.5 million be put to better use.

Management Decisions on OIG Recommendations That Funds Be Put to Better Use (Tables II-P and II-E)

In FY 2001, PCIE member agency management agreed with approximately \$22.1 billion in recommendations that funds be put to better use; ECIE member agency management agreed with approximately \$110.2 million in recommendations that funds be put to better use.

Questioned Costs (Tables III-P and III-E)

The IG Act defines a questioned cost as "a cost that is questioned by the Office because of (1) an alleged violation or provision of law, regulation, contract, grant, or cooperative agreement, or other agreement or document governing the expenditure of funds; (2) a finding that at the time of the audit, such cost is not supported by adequate documentation; or (3) a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable."

During FY 2001, including DCAA audits performed in agreement with OIGs or agencies, PCIE member agencies questioned costs of approximately \$3.9 billion; ECIE member agencies questioned costs of approximately \$233.3 million.

Management Decisions on Audits with Questioned Costs (Tables IV-P and IV-E)

For FY 2001, PCIE member agency management agreed with approximately \$2.3 billion in questioned costs; ECIE member agency management agreed with approximately \$24.9 million in questioned costs.

Both recommendations that funds be to better use and questioned costs can be resolved without an actual monetary recovery or reduction in outlays. In many cases, it is possible for management to take other corrective action to remedy or remove the condition that led to the auditor's finding. Consequently, the totals reported in these two categories do not represent a monetary savings to the Treasury in like amount.

Successful Criminal Prosecutions (Table V)

A prosecution is considered successful if the person or entity was convicted in a Federal, State, local, or foreign government venue, or under the Uniform Code of Military Justice (UCMJ), or was accepted for a pretrial diversion agreement by the DOJ as a result of OIG activity. PCIE and ECIE member agencies had 7,609 successful prosecutions in FY 2001, of which 108 were the result of joint investigations.

Criminal Indictments and Informations (Table VI)

This new table represents criminal indictments and informations filed in a Federal, State, local, or foreign government court or under the UCMJ, any of which result from a case in which an OIG has an active investigative role. The PCIE and ECIE agencies reported 4,980 criminal indictments and informations in FY 2001, of which 113 were based on joint investigations.

Civil Actions (Table VII)

Civil actions are the total number of matters arising from OIG investigations, audits, and reviews other than criminal prosecutions that are successfully resolved during the year. They include civil judgments or forfeitures in favor of the U.S. Government filed in Federal, State, local, or foreign government venues; or settlements negotiated by a prosecuting authority prior to or following the filing of a formal civil complaint; or judgments, settlements, or agreements reached based on Program Fraud Civil Remedies Act (PFCRA), Civil Monetary Penalty (CMP), or other agency-specific civil litigation authority. Personnel actions and suspensions/debarments are not reported as civil actions. In FY 2001, PCIE and ECIE member agencies had 905 civil actions, of which 4 resulted from joint investigations.

Suspensions and Debarments (Table VIII)

This category represents agency actions to suspend, restrict, or prohibit vendors/contractors, grantees, and other non-Government entities or individuals from doing business with the Government. In FY 2001, PCIE and ECIE member agencies suspended or debarred 8,828 individuals and entities, of which 28 actions resulted from joint investigations.

Personnel Actions (Table IX)

Personnel actions are the total number of reprimands, suspensions, demotions, or terminations of Federal, State, and local (and Federal contractor/grantee) employees as a result of OIG actions. During FY 2001, PCIE and ECIE member agencies initiated 1,213 personnel actions.

Investigative Recoveries (Table X)

Investigative recoveries are based on the total dollar value of:

1. Criminal cases—The amount of restitution, criminal fines, or special assessments resulting from a criminal judgment or established through a pretrial diversion agreement.
2. Civil cases—The amount of damages, penalties, or forfeitures resulting from judgments issued by any court (Federal, State, local, military, or foreign government) in favor of the U.S. Government; or the amount of funds to be repaid to the U.S. Government based on any negotiated settlements by a prosecuting authority; or the amount of any assessments or penalties imposed by PCFRA, CMP, or other agency-specific civil litigation authority.
3. Voluntary repayments—The amount of funds voluntarily repaid based on an OIG investigation before prosecutorial action is taken.

In FY 2001, PCIE and ECIE member agencies tallied investigative recoveries totaling \$3,748,150,897, of which \$152,729,630 resulted from joint investigations.

Collections from Audits and Investigations (Table XI)

Collections from audits and investigations are the total dollars collected or recovered during the FY that have been returned to the Treasury or the DOJ. In FY 2001, PCIE and ECIE audits collected \$526,130,683, while PCIE and ECIE investigations collected \$1,297,742,650.

Joint Investigations (Table XII)

This table lists the percentage of investigations PCIE and ECIE member agencies conducted with other Federal investigative entities, not including OIGs.

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

Agency	OIG	DCAA	Total
AID (Agency for International Development)	\$224,914,866	\$0	\$224,914,866
CNCS (Corporation for National and Community Service)	\$56,000	\$0	\$56,000
DOC (Department of Commerce)	\$14,188,794	\$0	\$14,188,794
DOD (Department of Defense)	\$413,454,000	\$3,139,100,000	\$3,552,554,000
DOE (Department of Energy)	\$1,274,658,923	\$0	\$1,274,658,923
DOI (Department of the Interior)	\$112,700,000	\$0	\$112,700,000
DOJ (Department of Justice)	\$24,323,109	\$0	\$24,323,109
DOL (Department of Labor)	\$2,348,180	\$0	\$2,348,180
DOS (Department of State)	\$522,000	\$0	\$522,000
DOT (Department of Transportation)	\$954,700,000	\$0	\$954,700,000
ED (Department of Education)	\$0	\$0	\$0
EPA (Environmental Protection Agency)	\$31,911,486	\$0	\$31,911,486
FDIC (Federal Deposit Insurance Corporation)	\$2,255,200	\$0	\$2,255,200
FEMA (Federal Emergency Management Agency)	\$11,888,621	\$0	\$11,888,621
GSA (General Services Administration)	\$90,841,259	\$216,000	\$91,057,259
HHS (Department of Health & Human Services)	\$63,118,166,000	\$0	\$63,118,166,000
HUD (Department of Housing & Urban Development)	\$4,095,000	\$0	\$4,095,000
NASA (National Aeronautics and Space Administration)	\$892,644,000	\$236,633,000	\$1,129,277,000
NRC (Nuclear Regulatory Commission)	\$75,000	\$0	\$75,000
OPM (Office of Personnel Management)	\$0	\$0	\$0
RRB (Railroad Retirement Board)	\$520,000	\$0	\$520,000
SBA (Small Business Administration)	\$11,061,994	\$0	\$11,061,994
SSA (Social Security Administration)	\$276,229,594	\$0	\$276,229,594
Treasury (Department of the Treasury) ¹	\$177,163,000	\$79,000	\$177,242,000
TIGTA (Treasury IG for Tax Administration)	\$13,000,326,022	\$0	\$13,000,326,022
TVA (Tennessee Valley Authority)	\$80,822,279	\$0	\$80,822,279
USDA (Department of Agriculture)	\$951,503,197	\$2,098,847	\$953,602,044
VA (Department of Veterans Affairs)	\$4,107,600,000	\$2,000,000	\$4,109,600,000
TOTALS	\$85,778,968,524	\$3,380,126,847	\$89,159,095,371
¹ Amount includes revenue enhancements of \$168,663,000. A revenue enhancement is an action recommended by Treasury OIG that would, if implemented, enhance the General Fund receipts of the Federal Government, usually without having any budgetary impact on any of the Department of the Treasury's appropriations.			

Table I-E: ECIE - Recommendations That Funds Be Put To Better Use

Agency	OIG	DCAA	Total
Amtrak	\$4,570,622	\$0	\$4,570,622
ARC (Appalachian Regional Commission)	\$5,666,000	\$0	\$5,666,000
CFTC (Commodity Futures Trading Commission)	\$0	\$0	\$0
CPB (Corporation for Public Broadcasting)	\$0	\$0	\$0
CPSC (Consumer Product Safety Commission)	\$0	\$0	\$0
EEOC (Equal Employment Opportunity Commission)	\$0	\$0	\$0
FCA (Farm Credit Administration)	\$0	\$0	\$0
FCC (Federal Communications Commission)	\$0	\$0	\$0
FEC (Federal Election Commission)	\$0	\$0	\$0
FHFB (Federal Housing Finance Board)	\$0	\$0	\$0
FLRA (Federal Labor Relations Authority)	n/a	n/a	n/a
FMC (Federal Maritime Commission)	\$0	\$0	\$0
FRB (Federal Reserve Board)	\$0	\$0	\$0
FTC (Federal Trade Commission)	\$29,359	\$0	\$29,359
GPO (Government Printing Office)	\$16,650	\$0	\$16,650
ITC (International Trade Commission)	\$78,537	\$0	\$78,537
LSC (Legal Services Corporation)	\$0	\$0	\$0
NARA (National Archives and Records Administration)	\$467,628	\$0	\$467,628
NCUA (National Credit Union Administration)	\$0	\$0	\$0
NEA (National Endowment for the Arts)	\$0	\$0	\$0
NEH (National Endowment for the Humanities)	\$0	\$0	\$0
NLRB (National Labor Relations Board)	\$0	\$0	\$0
NSF (National Science Foundation)	\$50,000	\$0	\$50,000
PBGC (Pension Benefit Guaranty Corporation)	\$0	\$0	\$0
PC (Peace Corps)	\$800	\$0	\$800
SEC (Securities and Exchange Commission)	\$0	\$0	\$0
SI (Smithsonian Institution)	\$381,960	\$0	\$381,960
USPS (U.S. Postal Service)	\$56,226,000	\$0	\$56,226,000
TOTAL	\$67,487,556	\$0	\$67,487,556

Table II-P: PCIE - Management Decisions on Recommendations That Funds Be Put To Better Use

Agency	No Management Decision Start FY 2001	Recommendations Issued in FY 2001	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 2001
AID	\$0	\$224,914,866	\$186,352,551	\$8,060,293	\$30,502,022
CNCS	\$0	\$56,000	\$0	\$0	\$56,000
DOC	\$157,989	\$14,188,794	\$2,153,872	\$5,643,127	\$6,549,846
DOD ¹	\$8,267,772,000	\$3,552,604,000	\$3,709,605,000	\$2,448,632,000	\$5,662,139,000
DOE	\$436,557,558	\$1,274,658,923	\$14,893,267	\$221,409,231	\$1,474,913,983
DOI ²	\$396,812,246	\$112,700,000	\$21,967,161	\$6,727,161	\$479,091,604
DOJ	\$265,210	\$24,323,109	\$11,309,337	\$0	\$13,278,982
DOL	\$7,987,478	\$2,348,180	\$6,723,129	\$1,079,349	\$2,533,180
DOS	\$1,447,000	\$522,000	\$428,000	\$0	\$1,541,000
DOT	\$137,702,000	\$954,700,000	\$966,700,000	\$76,000,000	\$49,702,000
ED	\$10,410,180	\$0	\$0	\$110,180	\$10,300,000
EPA	\$0	\$31,911,486	\$0	\$0	\$31,911,486
FDIC	\$0	\$2,255,200	\$2,255,200	\$0	\$0
FEMA	\$175,955,629	\$11,888,621	\$872,291	\$145,100,000	\$41,702,409
GSA ³	\$277,281,369	\$90,112,929	\$98,103,423	\$209,212,740	\$59,054,883
HHS ⁴	\$374,352,000	\$63,118,166,000	\$92,161,000	\$7,795,000	\$63,392,562,000
HUD	\$8,459,000	\$4,095,000	\$4,646,000	\$151,000	\$7,757,000
NASA ⁵	\$372,065,000	\$1,129,277,000	\$798,129,000	\$237,887,000	\$465,326,000
NRC	\$0	\$75,000	\$75,000	\$0	\$0
OPM	\$0	\$0	\$0	\$0	\$0
RRB	\$0	\$520,000	\$0	\$0	\$520,000
SBA ⁶	\$1,603,345	\$11,061,994	\$5,984,419	\$6,680,920	\$0
SSA	\$77,064,610	\$276,229,594	\$328,490,695	\$6,655,589	\$18,147,920
Treasury	\$17,122,000	\$177,242,000	\$189,943,000	\$4,342,000	\$79,000
TIGTA	\$9,186,160	\$13,000,326,022	\$13,008,445,717	\$968,056	\$98,409
TVA	\$0	\$80,822,279	\$47,604,447	\$32,882,582	\$335,250
USDA ⁷	\$808,846,056	\$953,602,044	\$121,887,296	\$1,479,266,680	\$161,239,622
VA	\$75,600,000	\$4,109,600,000	\$2,449,800,000	\$242,700,000	\$1,492,700,000
TOTALS	\$11,456,646,830	\$89,158,201,041	\$22,068,529,805	\$5,141,302,908	\$73,402,041,596

¹ Reflects a variance of \$1,941,528,000 (\$10,209,300,000 minus \$8,267,772,000) between the end of FY 2000 and the beginning of FY 2001 due to contracts not awarded and revised audit findings and recommendations.
² Reflects correction to data in FY 2000 PCIE-ECIE Report.
³ The difference between the amount in Recommendations Issued in FY 2001 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.
⁴ Start of FY 2001 differs from end of FY 2000 due to amendments in management decisions.
⁵ Start FY 2001 revised due to DCAA adjustments resulting from contracts not awarded and revised audit findings and recommendations.
⁶ Difference from September 2000 semi-annual report ending balance caused by prior reclassification of prior dollar finding from questioned cost to funds put to better use.
⁷ Reflects a variance of \$54,502 between beginning and ending balances due to the inclusion of excess amounts.

Table II-E: ECIE - Management Decisions On Recommendations That Funds Be Put To Better Use

Agency	No Management Decision Start FY 2001	Recommendations Issued in FY 2001	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 2001
Amtrak	\$0	\$4,570,622	\$1,480,525	\$67,602	\$3,022,495
ARC	\$298,000	\$5,666,000	\$1,254,000	\$2,544,000	\$2,166,000
CFTC	\$0	\$0	\$0	\$0	\$0
CPB	\$0	\$0	\$0	\$0	\$0
CPSC	\$0	\$0	\$0	\$0	\$0
EEOC	\$0	\$0	\$0	\$0	\$0
FCA	\$25,100	\$0	\$25,100	\$0	\$0
FCC	\$0	\$0	\$0	\$0	\$0
FEC	\$0	\$0	\$0	\$0	\$0
FHFB	\$10,000	\$0	\$0	\$10,000	\$0
FLRA	\$0	\$0	\$0	\$0	\$0
FMC	\$0	\$0	\$0	\$0	\$0
FRB	\$29,070	\$0	\$29,070	\$0	\$0
FTC	\$0	\$29,359	\$29,359	\$0	\$0
GPO	\$688,000	\$16,650	\$29,650	\$0	\$675,000
ITC	\$0	\$78,537	\$78,537	\$0	\$0
LSC	\$0	\$0	\$0	\$0	\$0
NARA	\$0	\$467,628	\$0	\$0	\$467,628
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	\$0	\$50,000	\$0	\$0	\$50,000
PBGC	\$0	\$0	\$0	\$0	\$0
PC ¹	\$2,000	\$800	\$2,800	\$0	\$0
SEC	\$0	\$0	\$0	\$0	\$0
SI	\$109,261	\$381,960	\$11,052	\$0	\$480,169
USPS	\$108,132,118	\$56,225,711	\$107,314,035	\$8,502,504	\$48,541,290
TOTALS	\$109,293,549	\$67,487,267	\$110,254,128	\$11,124,106	\$55,402,582
¹ Reflects correction to data in FY 2000 PCIE-ECIE Report.					

Table III-P: PCIE - Questioned Costs

Agency	OIG	DCAA	Total
AID	\$5,946,950	\$2,528,072	\$8,475,022
CNCS	\$2,984,000	\$0	\$2,984,000
DOC	\$10,638,410	\$0	\$10,638,410
DOD	\$0	\$1,410,900,000	\$1,410,900,000
DOE ¹	\$7,651,747	\$0	\$7,651,747
DOI	\$15,788,601	\$0	\$15,788,601
DOJ	\$142,371,705	\$0	\$142,371,705
DOL	\$41,641,821	\$0	\$41,641,821
DOS	\$11,500,000	\$0	\$11,500,000
DOT	\$72,244,000	\$0	\$72,244,000
ED	\$82,435,089	\$0	\$82,435,089
EPA	\$29,050,869	\$2,173,495	\$31,224,364
FDIC	\$5,708,216	\$0	\$5,708,216
FEMA	\$42,252,923	\$0	\$42,252,923
GSA	\$11,542,604	\$0	\$11,542,604
HHS	\$1,008,237,000	\$0	\$1,008,237,000
HUD	\$85,155,000	\$0	\$85,155,000
NASA	\$0	\$30,676,000	\$30,676,000
NRC	\$0	\$2,422	\$2,422
OPM	\$279,650,719	\$0	\$279,650,719
RRB	\$0	\$0	\$0
SBA	\$520,673	\$0	\$520,673
SSA	\$135,100,905	\$0	\$135,100,905
Treasury	\$0	\$1,266,000	\$1,266,000
TIGTA	\$715	\$167,713	\$168,428
TVA	\$6,131,711	\$0	\$6,131,711
USDA ²	\$423,876,783	\$440	\$423,877,223
VA	\$24,400,000	\$0	\$24,400,000
TOTALS	\$2,444,830,441	\$1,447,714,142	\$3,892,544,583
¹ The Energy OIG's submission does not include nor does it track DCAA audits			
² Includes \$1,671,339 in recommendations from work performed by non-Federal auditors.			

Table III-E: ECIE - Questioned Costs

Agency	OIG	DCAA	Total
Amtrak	\$17,304,505	n/a	\$17,304,505
ARC	\$250,000	n/a	\$250,000
CFTC	\$0	\$0	\$0
CPB	\$786,131	\$0	\$786,131
CPSC	\$0	\$0	\$0
EEOC	\$0	\$0	\$0
FCA	\$0	\$0	\$0
FCC	\$1,324,977	\$0	\$1,324,977
FEC	\$0	\$0	\$0
FHFB	\$0	\$0	\$0
FLRA	n/a	n/a	\$0
FMC	\$0	\$0	\$0
FRB	\$0	\$0	\$0
FTC	\$189,202	\$0	\$189,202
GPO	\$148,548	n/a	\$148,548
ITC	\$1,000	\$0	\$1,000
LSC	\$0	\$0	\$0
NARA	\$1,314,332	\$0	\$1,314,332
NCUA	\$0	\$0	\$0
NEA	\$25,181	\$0	\$25,181
NEH	n/a	n/a	\$0
NLRB	\$0	\$0	\$0
NSF	\$6,377,345	\$11,297	\$6,388,642
PBGC	\$0	\$0	\$0
PC	\$9,614	\$0	\$9,614
SEC	\$0	\$0	\$0
SI	\$0	\$0	\$0
USPS	\$131,273,000	\$74,323,000	\$205,596,000
TOTALS	\$159,003,835	\$74,334,297	\$233,338,132

Table IV-P: PCIE - Management Decisions on Audits With Questioned Costs

Agency	No Management Decision Start FY 2001	Recommendations Issued in FY 2001	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 2001
AID ¹	\$59,639,930	\$8,475,022	\$13,970,555	\$52,053,375	\$2,091,022
CNCS	\$10,408,000	\$2,984,000	\$650,000	\$145,000	\$12,597,000
DOC	\$4,675,622	\$10,638,410	\$7,491,950	\$3,668,326	\$4,189,759
DOD ²	\$7,409,800,000	\$1,410,900,000	\$961,800,000	\$533,000,000	\$7,325,900,000
DOE	\$7,651,747	\$0	\$0	\$0	\$7,651,747
DOI ³	\$185,900,170	\$15,788,601	\$2,047,827	\$732,158	\$193,712,749
DOJ	\$10,210,766	\$142,371,705	\$111,529,629	\$0	\$41,052,842
DOL	\$53,480,804	\$41,641,821	\$6,874,251	\$7,286,436	\$80,978,425
DOS ⁴	\$6,775,000	\$11,500,000	\$860,000	\$0	\$17,415,000
DOT ⁵	\$427,000	\$72,244,000	\$64,679,000	\$42,000	\$8,078,000
ED ⁶	\$116,476,150	\$82,435,089	\$21,504,102	\$15,868,072	\$161,539,065
EPA ⁷	\$103,224,369	\$31,224,364	\$59,504,639	\$23,331,024	\$51,613,070
FDIC	\$0	\$5,708,216	\$5,708,216	\$0	\$0
FEMA	\$35,901,096	\$42,252,923	\$19,206,340	\$17,998,634	\$40,949,045
GSA ⁸	\$2,802,975	\$11,542,604	\$14,667,826	\$549,509	\$349,043
HHS ⁹	\$653,719,000	\$1,008,237,000	\$411,081,000	\$36,315,000	\$1,214,560,000
HUD	\$43,715,000	\$85,155,000	\$59,979,000	\$4,731,000	\$64,160,000
NASA ¹⁰	\$234,727,000	\$30,676,000	\$30,801,000	\$23,697,000	\$210,905,000
NRC	\$0	\$2,422	\$2,422	\$0	\$0
OPM	\$65,673,570	\$279,650,719	\$233,572,058	\$42,825,087	\$68,927,144
RRB	\$0	\$0	\$0	\$0	\$0
SBA ¹¹	\$4,046,779	\$520,673	\$3,622,085	\$581,236	\$573,482
SSA	\$81,148,807	\$135,100,905	\$212,224,763	\$512,102	\$3,512,847
Treasury ¹²	\$4,032,000	\$1,266,000	\$1,141,000	\$1,739,000	\$2,418,000
TIGTA	\$0	\$168,428	\$32,537	\$0	\$135,891
TVA	\$1,409,712	\$6,131,711	\$4,245,821	\$3,192,049	\$103,553
USDA ¹³	\$2,101,833,748	\$423,877,223	\$45,387,747	\$2,267,744,027	\$213,449,337
VA	\$0	\$24,400,000	\$24,400,000	\$0	\$0
TOTALS	\$11,197,679,245	\$3,884,892,836	\$2,316,983,768	\$3,036,011,035	\$9,726,862,021

¹ The ending balance for fiscal year 2000 of \$59,599,349 was increased by \$40,581 to reflect adjustments in finding amounts occurring in five reports within FY 2002 reporting period \$59,639,930.

² Includes forward pricing proposals and operations audits. Reflects a variance of \$687,300,000 (\$8,097,100,000 minus \$7,409,800,000) between the end of FY 2000 and the beginning of FY 2001 due to contracts not awarded and revised audit findings and recommendations.

³ Reflects correction to data in FY 2000 PCIE-ECIE Report.

⁴ Start FY 2001 differs from end of FY 2000 due to post-reporting period corrections.

⁵ Dollar Value of Disallowed Costs includes \$128,000 that management decided to seek above recommended amounts.

⁶ Reflects corrections to data in FY 2000 PCIE-ECIE Report, which are detailed in ED semi-annual reports 42 and 43 for FY 2001.

⁷ Start FY 2001 differs from end of FY 2000 due to post-reporting period adjustments.

⁸ Includes \$1,220,799 that management decided to seek that exceeded recommended amounts.

⁹ Start of FY 2001 differs from end of FY 2000 due to amendments in management decisions.

¹⁰ Start FY 2001 revised due to DCAA adjustments resulting from contracts not awarded and revised audit findings and recommendations.

¹¹ Difference from September 2000 semi-annual report ending balance caused by prior reclassification of prior dollar finding from questioned cost to funds put to better use.

¹² For two reports, management partially agreed to the dollar value of the recommendations.

¹³ Reflects the decrease of one audit and \$240,769 for adjustments made between the first and second semiannual periods during fiscal year 2001. Reflects a variance of \$1,110,909 between the beginning and ending balance because of the inclusion of excess amounts.

Table IV-E: ECIE - Management Decisions On Audits With Questioned Costs

Agency	No Management Decision Start FY 2001	Recommendations Issued in FY 2001	Recommendations Agreed to by Management	Recommendations Not Agreed to by Management	No Management Decision End FY 2001
Amtrak	\$923,674	\$17,304,504	\$15,066,376	\$801,090	\$2,360,712
ARC	\$133,000	\$250,000	\$1,000	\$354,000	\$28,000
CFTC	\$0	\$0	\$0	\$0	\$0
CPB	\$109,969	\$786,131	\$0	\$109,969	\$786,131
CPSC	\$0	\$0	\$0	\$0	\$0
EEOC	\$0	\$0	\$0	\$0	\$0
FCA	\$0	\$0	\$0	\$0	\$0
FCC	\$265,180	\$1,342,977	\$135,180	\$130,000	\$1,342,977
FEC	\$0	\$0	\$0	\$0	\$0
FHFB	\$0	\$0	\$0	\$0	\$0
FLRA	n/a	n/a	n/a	n/a	n/a
FMC	\$0	\$0	\$0	\$0	\$0
FRB	\$0	\$0	\$0	\$0	\$0
FTC	\$0	\$189,202	\$189,202	\$0	\$0
GPO	\$361,101	\$123,895	\$362,505	\$122,491	\$0
ITC	\$0	\$1,000	\$1,000	\$0	\$0
LSC	\$0	\$0	\$0	\$0	\$0
NARA	\$0	\$1,314,332	\$1,314,332	\$0	\$0
NCUA	\$0	\$0	\$0	\$0	\$0
NEA	\$309,174	\$25,181	\$309,174	\$0	\$25,181
NEH	n/a	n/a	n/a	n/a	n/a
NLRB	\$0	\$0	\$0	\$0	\$0
NSF	\$6,000,536	\$6,388,642	\$1,888,877	\$5,248,282	\$5,389,095
PBGC	\$0	\$0	\$0	\$0	\$0
PC	\$0	\$9,614	\$0	\$9,614	\$0
SEC	\$0	\$0	\$0	\$0	\$0
SI	\$0	\$0	\$0	\$0	\$0
USPS	\$76,890,998	\$205,596,276	\$5,680,634	\$9,509,423	\$267,297,217
TOTALS	\$84,993,632	\$233,331,754	\$24,948,280	\$16,284,869	\$277,229,313

Table V: Successful Criminal Prosecutions

PCIE		ECIE	
Agency	Total	Agency	Total
AID	9	Amtrak	20
CNCS	4	ARC	0
DOC	8	CFTC	0
DOD	244	CPSC	0
DOE	10	CPB	0
DOI	31	EEOC	0
DOJ	133	FCA	0
DOL	215	FCC	0
DOS	29	FEC	0
DOT	147	FHFB	0
ED	91	FLRA	0
EPA	23	FMC	0
FDIC	24	FRB	1
FEMA	32	FTC	0
GSA	35	GPO	1
HHS	406	ITC	0
HUD	727	LSC	1
NASA	42	NARA	0
NRC	7	NCUA	0
OPM	19	NEA	0
RRB	51	NEH	0
SBA	37	NLRB	0
SSA ¹	4,190	NSF	2
Treasury	4	PBGC	1
TIGTA	243	PC	4
TVA	10	SEC	0
USDA ²	352	SI	1
VA	318	USPS ³	29
SUBTOTAL	7,441	SUBTOTAL	60
TOTAL FROM INDIVIDUAL INVESTIGATIONS: 7,501			
TOTAL FROM JOINT INVESTIGATIONS: 108			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: 7,609			
¹ Includes 2,158 fugitive felon and 656 illegal alien apprehensions.			
² Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			
³ During FY 2001, the USPS Inspection Service had 480 successful prosecutions that are reported in the Postal Service OIG's semiannual reports to Congress. These prosecutions include matters where concurrent jurisdiction existed, as well as matters for which the Inspection Service has primary responsibility.			

Table VI: Criminal Indictments and Informations

PCIE		ECIE	
Agency	Total	Agency	Total
AID	6	Amtrak	0
CNCS	0	ARC	0
DOC	0	CFTC	0
DOD	312	CPSC	0
DOE	4	CPB	0
DOI	25	EEOC	0
DOJ	153	FCA	0
DOL	359	FCC	0
DOS	21	FEC	0
DOT	186	FHFB	0
ED	125	FLRA	0
EPA	14	FMC	0
FDIC	28	FRB	1
FEMA	53	FTC	0
GSA	33	GPO	0
HHS	515	ITC	0
HUD	778	LSC	0
NASA	34	NARA	0
NRC	0	NCUA	0
OPM	19	NEA	0
RRB	36	NEH	0
SBA	38	NLRB	0
SSA	1,122	NSF	0
Treasury	1	PBGC	0
TIGTA	236	PC	0
TVA	13	SEC	0
USDA ¹	358	SI	4
VA	359	USPS	34
SUBTOTAL	4,828	SUBTOTAL	39
TOTAL FROM INDIVIDUAL INVESTIGATIONS: 4,867			
TOTAL FROM JOINT INVESTIGATIONS: 113			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: 4,980			
¹ Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			

Table VII: Civil Actions

PCIE		ECIE	
Agency	Total	Agency	Total
AID	2	Amtrak	0
CNCS	2	ARC	0
DOC	0	CFTC	0
DOD	7	CPSC	0
DOE	4	CPB	0
DOI	9	EEOC	0
DOJ	2	FCA	0
DOL	28	FCC	0
DOS	1	FEC	0
DOT	12	FHFB	0
ED ¹	137	FLRA	0
EPA	3	FMC	0
FDIC	6	FRB	0
FEMA	6	FTC	0
GSA	5	GPO	0
HHS	416	ITC	0
HUD	21	LSC	0
NASA	8	NARA	0
NRC	1	NCUA	0
OPM	7	NEA	0
RRB	53	NEH	0
SBA	7	NLRB	0
SSA	72	NSF	1
Treasury	0	PBGC	0
TIGTA	0	PC	0
TVA	2	SEC	0
USDA ¹	78	SI	0
VA	9	USPS	2
Subtotal	898	Subtotal	3
TOTAL FROM INDIVIDUAL INVESTIGATIONS: 901			
TOTAL FROM JOINT INVESTIGATIONS: 4			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: 905			
¹ Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			

Table VIII: Suspensions and Debarments

PCIE		ECIE	
Agency	Total	Agency	Total
AID	5	Amtrak	0
CNCS	2	ARC	0
DOC	0	CFTC	0
DOD	243	CPSC	0
DOE	11	CPB	0
DOI	3	EEOC	0
DOJ	1	FCA	0
DOL	29	FCC	0
DOS	0	FEC	0
DOT	17	FHFB	0
ED	0	FLRA	0
EPA	11	FMC	0
FDIC	0	FRB	0
FEMA	0	FTC	0
GSA	94	GPO	4
HHS	3,752	ITC	0
HUD	418	LSC	0
NASA	7	NARA	0
NRC	4	NCUA	0
OPM	4,033	NEA	0
RRB	0	NEH	0
SBA	0	NLRB	0
SSA	0	NSF	0
Treasury	0	PBGC	0
TIGTA	0	PC	0
TVA	0	SEC	0
USDA ¹	153	SI	0
VA	11	USPS	2
SUBTOTAL	8,794	SUBTOTAL	6
TOTAL FROM INDIVIDUAL INVESTIGATIONS: 8,800			
TOTAL FROM JOINT INVESTIGATIONS: 28			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: 8,828			
¹ Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			

Table IX: Personnel Actions

PCIE		ECIE	
Agency	Total	Agency	Total
AID	10	Amtrak	74
CNCS ¹	11	ARC	0
DOC ¹	11	CFTC	0
DOD	23	CPSC	0
DOE	16	CPB	0
DOI	85	EEOC	0
DOJ	82	FCA	0
DOL	29	FCC	0
DOS	5	FEC	0
DOT	20	FHFB	1
ED	2	FLRA	0
EPA	7	FMC	0
FDIC	0	FRB	11
FEMA	7	FTC	1
GSA	18	GPO	9
HHS	2	ITC	0
HUD	0	LSC	0
NASA	26	NARA	4
NRC	20	NCUA	4
OPM	0	NEA	0
RRB	0	NEH	0
SBA	6	NLRB	5
SSA	18	NSF	2
Treasury	13	PBGC	13
TIGTA	420	PC	5
TVA	30	SEC	5
USDA ¹	57	SI	12
VA	133	USPS	16
SUBTOTAL	1,051	SUBTOTAL	162
TOTAL FROM INDIVIDUAL INVESTIGATIONS: 1,213			
TOTAL FROM JOINT INVESTIGATIONS: 0			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: 1,213			
¹ Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			

Table X: Investigative Recoveries

PCIE		ECIE	
Agency	Total	Agency	Total
AID	\$67,248,547	Amtrak	\$591,400
CNCS	\$54,102	ARC	\$0
DOC ¹	\$73,429	CFTC	\$0
DOD	\$1,394,090,677	CPSC	\$0
DOE	\$5,408,770	CPB	\$0
DOI	\$156,594,774	EEOC	\$0
DOJ	\$989,047	FCA	\$0
DOL	\$101,313,740	FCC	\$0
DOS	\$414,701	FEC	\$0
DOT	\$62,615,348	FHFB	\$0
ED ¹	\$21,642,373	FLRA	\$0
EPA	\$4,386,638	FMC	\$0
FDIC	\$78,848,150	FRB	\$525
FEMA	\$3,209,244	FTC	\$0
GSA	\$4,520,706	GPO	\$35,315
HHS	\$1,374,087,301	ITC	\$0
HUD	\$61,012,560	LSC	\$12,000
NASA	\$67,651,346	NARA	\$0
NRC	\$2,786,802	NCUA	\$0
OPM	\$7,913,317	NEA	\$0
RRB	\$2,423,944	NEH	\$0
SBA	\$11,624,713	NLRB	\$40
SSA	\$44,023,673	NSF	\$424,578
Treasury	\$214,127	PBGC	\$300
TIGTA	\$13,352,162	PC	\$0
TVA	\$5,997,628	SEC	\$0
USDA ¹	\$61,893,678	SI	\$42,743
VA	\$35,189,396	USPS	\$4,733,473
SUBTOTAL	\$3,589,580,893	SUBTOTAL	\$5,840,374
TOTAL FROM INDIVIDUAL INVESTIGATIONS: \$3,595,421,267			
TOTAL FROM JOINT INVESTIGATIONS: \$152,729,630			
TOTAL FROM INDIVIDUAL AND JOINT INVESTIGATIONS: \$3,748,150,897			
¹ Data provided by OIG and could not be included in the IG community's project to identify duplicate reporting.			

Table XI: PCIE and ECIE - Collections From Audits and Investigations

PCIE	From Audits	From Investigations	ECIE	From Audits	From Investigations
AID	\$28,549,000	\$66,355,660	Amtrak	\$11,583,084	\$113,229
CNCS	\$0	\$39,393	ARC	n/a	n/a
DOC	\$6,875,989	\$21,911	CFTC	\$0	\$0
DOD	\$0	\$0	CPB	n/a	\$0
DOE	\$0	\$13,264,088	CPSC	\$0	\$0
DOI	\$0	\$0	EEOC	\$0	\$0
DOJ	\$6,845,260	\$108,827	FCA	\$0	\$0
DOL	\$1,073,929	\$926,717	FCC	\$0	\$0
DOS	n/a	\$440,310	FEC	\$0	\$0
DOT	n/a	n/a	FHFB	\$0	\$0
ED	\$1,905,940	\$869,282	FLRA	\$0	\$0
EPA	\$0	\$0	FMC	\$0	\$0
FDIC	\$0	\$0	FRB	\$0	\$0
FEMA	\$17,246,807	\$0	FTC	\$674,500	\$0
GSA	\$0	\$0	GPO	\$0	\$0
HHS	\$315,835,000	\$1,083,209,720	ITC	\$0	\$0
HUD	\$6,089,748	\$52,149,893	LSC	\$0	\$0
NASA	\$0	\$4,342,601	NARA	\$0	\$0
NRC	\$0	\$2,767,262	NCUA	\$0	\$0
OPM	\$102,064,000	\$7,768,805	NEA	\$0	\$0
RRB	\$0	\$990,356	NEH	n/a	n/a
SBA	\$0	\$0	NLRB	\$0	\$0
SSA	\$2,039,707	\$15,271,127	NSF	\$1,496,529	n/a
Treasury	\$8,579,100	n/a	PBGC	\$0	\$0
TIGTA	\$0	\$119,375	PC	\$0	\$0
TVA	\$0	\$123,935	SEC	\$0	\$0
USDA	\$15,251,631	\$20,772,858	SI	\$0	\$0
VA	\$20,459	\$24,509,301	USPS	\$0	\$3,578,000
SUBTOTAL	\$512,376,570	\$1,294,051,421	SUBTOTAL	\$13,754,113	\$3,691,229
TOTAL PCIE/ECIE Audit		\$526,130,683	TOTAL PCIE/ECIE Investigation		\$1,297,742,650

Table XII: PCIE and ECIE - Joint Investigations

PCIE	Percentage of Investigations conducted with other Federal Investigative Offices not including OIGs	ECIE	Percentage of Investigations conducted with other Federal Investigative Offices not including OIGs
AID	2%	Amtrak	n/a
CNCS	0%	ARC	n/a
DOC	100%	CFTC	0%
DOD	55%	CPB	0%
DOE	24%	CPSC	0%
DOI	0%	EEOC	10%
DOJ	18%	FCA	0%
DOL	11%	FCC	16%
DOS	43%	FEC	0%
DOT	16%	FHFB	0%
ED	13%	FLRA	0%
EPA	0%	FMC	0%
FDIC	33%	FRB	0%
FEMA	15%	FTC	100%
GSA	19%	GPO	0%
HHS	0%	ITC	0%
HUD	30%	LSC	0%
NASA	34%	NARA	20%
NRC	0%	NCUA	0%
OPM	61%	NEA	0%
RRB	5%	NEH	0%
SBA	21%	NLRB	0%
SSA	7%	NSF	17%
Treasury	0%	PBGC	0%
TIGTA	1%	PC	0%
TVA	0%	SEC	8%
USDA	9%	SI	10%
VA	28%	USPS	10%

A Compendium of OIG Activities in FY 2001

OIGs provide a valuable service with their audits, investigations, inspections, and other initiatives. Governmentwide, there are many excellent examples of the critical work performed by OIGs. The many accomplishments of the OIGs are too numerous to include, so a representative sample was selected for inclusion in this report. These examples focus on issues that reflect current priorities of the Federal Government or interests of the general public.

The IG Community's Response to the September 11 Terrorist Attacks

As the Office of Homeland Security recently stated in its "Securing the Homeland, Strengthening the Nation" report, "The United States Government has no more important mission than fighting terrorism overseas and securing the homeland from future terrorist attacks." OIGs across the Federal Government have taken this challenge very seriously.

In the weeks following the tragic events of September 11, many questions were asked about the terrorists. How were they able to assimilate themselves into our society? What documentation did they have, and how did they obtain it? How were they able to finance their operations? Were their supporters in the United States? The list continues. In response to these questions and others, the IG community rose to the challenge and provided assistance and support in numerous areas.

We are committed to providing whatever assistance we can to bring to justice those who committed the unfathomable terrorist acts against our Nation. Additionally, we will provide whatever knowledge and resources we have to effect significant changes in our Federal programs, so terrorists cannot use our own systems and processes against us.

As evidenced by the myriad efforts OIGs have already taken, both collaboratively and individually, our resolve is deep. A summary of these efforts follows.

Rescue and Evidence Recovery

Immediately following the attacks, hundreds of OIG special agents and other personnel participated in rescue and evidence recovery efforts at the World Trade Center, the Pentagon, and the Pennsylvania crash site. For example, the Defense Criminal Investigative Service (DCIS), the criminal investigative arm of the DOD OIG, assisted in initial search and rescue efforts soon after American Airlines Flight 77 struck the Pentagon. Working with the FBI task force, DCIS agents arranged for a temporary morgue at a National Guard Center and a storage site for recovered aircraft pieces at an Army Reserve Center, both near the Pennsylvania crash site.

The DOJ OIG provided 29 people to assist the New York Port Authority Police, the FBI, and the Federal Aviation Administration (FAA) in their rescue, evidence recovery, and investigative efforts during the weeks following the attacks. Immediately following the attacks, U.S. Postal Service (USPS) OIG agents assisted the New York/New Jersey Port Authority in securing the safe transportation of people to and from the lower Manhattan area via the New York/New Jersey waterways. Before September 11, the waterways averaged 32,000 passengers per day, but on September 11, OIG agents helped evacuate more than 160,000 people from New York to New Jersey.

Numerous OIGs, including DOD, DOE, DOJ, Treasury, USDA, the Departments of Commerce (DOC), Education (ED), Housing and Urban Development (HUD), Labor (DOL), State (DOS), and Veterans Affairs (VA), as well as USPS, NASA, SSA, TIGTA, EPA, OPM, Farm Credit Administration (FCA), Federal Deposit Insurance Corporation (FDIC), Equal Employment Opportunity Commission (EEOC), National Credit Union Administration (NCUA), Amtrak, the Government Printing Office (GPO), and the General Services Administration (GSA), sent teams of special agents to the Pentagon and World

Trade Center to assist in evidence recovery. Typically, the agents worked 12-hour shifts to sift through debris and rubble in search of airplane parts and evidence that would identify the victims.

Investigative Assistance and Participation in Antiterrorism Task Forces

OIG special agents across the country assisted FBI and other law enforcement agencies after the terrorist attacks by doing what they do best—attempting to put together the pieces of an elaborate and dangerous puzzle. Almost every IG provided investigative assistance and resources to:

- Identify, interview, and arrest criminal suspects.
- Trace funds.
- Conduct record checks, searches, and surveillance.
- Provide computer forensic support.

For example, several OIGs detailed special agents to the FBI's National Infrastructure Protection Center to assist in certain aspects of the investigation. In fact, one ED OIG special agent became a shift leader in the FBI's Headquarters Technology Cell, where he provided oversight in processing electronic evidence such as questionable e-mail accounts, flight records, and seized computers. Using advanced technology, the Cell found online clues to assist in charting the conspirators' actions.

SSA OIG's involvement in the ongoing national investigation has grown daily since September 11. This involvement is mandated by the role the SSN plays in establishing false identities and committing the financial crimes necessary to bankroll terrorism. Nine SSA OIG special agents in the New York and New Jersey area were assigned exclusively to the FBI investigation.

In addition, one SSA OIG agent was quickly assigned to the FBI's Strategic Information and Operations Center and another to the National Infrastructure Protection Center. Six members of SSA OIG's Electronic Crimes Team assisted the FBI, while two computer specialists wrote programs to query SSA's databases more specifically for information the FBI needed. Seven additional agents fielded requests for SSN information on suspects and witnesses, each of which was routed through the FBI's Baltimore office to SSA headquarters. Many of SSA OIG's special agents are working full time on the terrorism investigation and responding to allegations of SSN misuse.

Many IGs have also committed resources to participate in national and State terrorism task forces, such as the FBI's Joint Terrorism Task Force (JTTF), which is designed to use their collective resources to prevent, preempt, deter, and investigate terrorism and activities related to terrorism. Several IGs have contributed significantly to the FBI's anthrax and bioterrorism investigation. USPS OIG participated on FBI task forces to help identify potential suspects and assisted the Inspection Service in screening and investigating suspicious mail to maintain the integrity of the Nation's mail system.

USDA OIG special agents visited 51 USDA-owned or -sponsored laboratories and research facilities across the United States to evaluate their vulnerability to terrorism. OIG special agents have responded to and conducted numerous investigations involving biological threats at USDA-owned or -regulated facilities or threats made by USDA employees. In fact, several USDA employees are facing potential criminal prosecution and/or agency personnel action for anthrax hoaxes and false reports of possible food contamination at USDA-inspected plants.

Air Marshal Program

The FAA requested special agents from the Federal law enforcement community to be temporarily detailed to its Federal Air Marshal program for 6 to 18 months. OPM's OIG coordinated the IG

community's response to the FAA. More than 15 OIGs responded to the call for assistance with a number of special agents, even though they also had committed other special agent resources to assist the FBI in New York. Numerous OIG staff from organizations such as Treasury, VA, ED, DOC, DOE, DOJ, DOT, HHS, the Small Business Administration (SBA), and GSA have been detailed to the FAA Air Marshal Service while it expands its permanent cadre.

Security of Agency Personnel and Facilities

Following the September 11 attacks, several OIGs assigned special agents to provide security for Federal leaders, personnel, and facilities. For example, the Secretary of Labor asked its OIG to take over the security of departmental facilities on a temporary basis to assess security, identify vulnerabilities, recommend solutions, and enhance the technical expertise of departmental staff. Because disruption of the U.S. Government appears to be one goal of terrorism, the USDA OIG heightened its protection of the Secretary and joined in ensuring the continuation of USDA functions in the event of further assaults.

Other Initiatives

OIGs throughout the Government recognized after the September 11 attacks that securing our country and finding those responsible were our immediate priorities. Equally important, however, was determining how the terrorists committed these offenses.

With this information, OIGs could make recommendations to their respective agencies regarding the implementation of controls and processes to address systemic vulnerabilities that failed to prevent and detect the crimes or even facilitated their occurrence. Many OIGs refocused their planned audit initiatives for FY 2002 to items that had more immediate importance for preventing future terrorist attacks and protecting citizens and Federal employees. Several examples are highlighted below.

DOE's OIG reevaluated its FY 2002 work plan in view of the issues and vulnerabilities that surfaced as a result of the attacks. Given the implications with regard to DOE operations and programs, OIG shifted a significant amount of its planned resources to examine related topics.

Specific planned initiatives include reviews of the security of the DOE's aircraft and the adequacy of the hiring process for drivers who transport hazardous and low-level waste. OIG also initiated several follow-up reviews to evaluate the actions DOE has taken to correct previously identified security concerns in areas such as the following:

- Classified document mailings.
- Coordination of transportation safeguard activities.
- Export controls relating to foreign visits and assignments.

EPA OIG added "Protecting Infrastructure from Nontraditional Attacks" to its list of management challenges, recognizing that the Nation's water supply, among other targets, could be vulnerable to a terrorist attack. EPA has created an action plan to address threats to public health through environmental resources. OIG reported this as a major management challenge to ensure that actions are taken and milestones are met to protect infrastructure.

FDIC's OIG began evaluating the adequacy of physical security in its facilities in major cities and other selected sites throughout the country. The evaluation placed particular emphasis on the security measures taken to provide a safe work environment for FDIC employees and visitors. The review was designed to determine whether FDIC's safety and environmental management policies for real property had been established and implemented to:

- Protect Federal real and personal property.
- Promote mission continuity.
- Assess risk.
- Make decisionmakers aware of risks.
- Act promptly and appropriately in response to risk.

HHS' OIG is currently assessing State and local health departments' ability to detect and respond to bioterrorism and to deploy medical supplies. In addition, OIG plans to evaluate the vaccine procurement program and adherence to regulations governing facilities that transfer and receive select agents, which have the potential to pose a severe threat to public health and safety, and could be used as weapons of mass destruction for criminal or terrorist purposes.

In light of the events of September 11, DOJ OIG initiated five follow-up reviews at the Immigration and Naturalization Service (INS), whose work is critical to deterring terrorists from entering or remaining in the United States. DOJ OIG examined INS progress in:

- Improving the Visa Waiver Program.
- Securing the northern border.
- Linking INS and FBI automated fingerprint identification systems.
- Implementing a reliable tracking system for nonimmigrants who overstay their visas.
- Reviewing security concerns regarding the Transit Without Visa Program.

Findings from all five follow-up reviews show that many of the security concerns identified in the original DOJ OIG reports persist.

As stated earlier, SSA OIG immediately began preparing information that Congress used to craft antiterrorism legislation since the attacks. OIG gave Congress an assessment of SSA's business processes for issuing and protecting SSNs. This assessment covered areas such as:

- Securing valid evidence presented with SSN applications.
- Computerized controls.
- Training for SSA employees.
- SSA's accounting for SSN cards.
- Public awareness of the proper use and dissemination of the SSN.
- SSA's coordination efforts with other Federal agencies.

OIG also provided an assessment to Congress of SSA's programs and operations to identify fake and stolen SSN cards and described SSA's coordination efforts with other Federal agencies to identify suspected terrorists. In November, OIG provided Congress with its opinion on new techniques—such as new categories of SSNs, photo identification cards, and additional automated controls—to improve SSN verification and decrease incidents of identity theft. This work continued into FY 2002.

Throughout SSA OIG's responses to Congress, OIG relayed the importance of limiting the role of the SSN by stopping the commercial use of SSNs by institutions such as schools and hospitals, and regulating the sale and purchase of SSNs. Also, OIG has reiterated its position that SSA needs to strengthen its business processes, including interagency data verification and data matching agreements between Federal and State agencies, to prevent future fraudulent activities that may aid

terrorists. In particular, SSA OIG strongly encouraged SSA to pursue matching agreements with States that use biometric technology.

The following table summarizes the IG community's participation in activities immediately following September 11.

IG Community Participation Following September 11, 2001						
		AGENCY SUPPORTED			TYPES OF DUTY	
AGENCY	PERSONNEL	FBI (Hours)	FAA (Hours)	TOTAL HRS	INVESTIGATIVE	EVIDENCE RECOVERY
Agriculture	95	5,927		5,927	X	X
AID	1	60	60	120	X	
AMTRAK	1	40		40		X
DCIS	125	30,000		30,000	X	X
DOC	5	709	161	870	X	X
DOE	22	1,607		1,607	X	
DOI	10	1,193		1,193	X	
DOJ	29	2,850	1,089	3,940	X	X
DOL	46	3,333		3,333	X	X
DOS	3	92		92	X	X
DOT	44	9,004	3,108	12,112	X	
ED	35	2,475	420	2,895	X	X
EEOC	2	112		112		X
EPA	3	106		106		X
FCA	1	48		48		X
FDIC	10	612		612	X	X
GPO	7	1,071		1,071	X	X
GSA	9	1,839		1,839	X	
HHS	7	838		838	X	
HUD	97	7,650	4,512	12,162	X	X
NASA	13	1,397		1,397	X	X
NCUA	1	24		24		X
NRC	2	446		446	X	
NSF	2	140		140	X	X
OPM	2	170		170	X	X
RRB	10	983		983	X	
SBA	3	519	211	730	X	
SSA	207	13,000		13,000	X	X
TIGTA	110	23,106	2,100	25,206	X	X
Treasury	7	810	768	1,578	X	X
USPS	26	2,089		2,089	X	X
VA	34	8,086		8,086	X	X
TOTAL	32	120,336	12,429	132,766	28	24

Focus on Agency Management Challenges Aligns With the President's Management Agenda

For the fourth consecutive year, OIGs across the Federal Government have examined their agencies' programs and operations and shared their agencies' top management challenges with congressional leaders. OIGs identified these challenges through ongoing work related to each agency's overall mission and discussed how the issues unique to their agencies would be addressed.

With their focus on activities that promote Governmentwide efficiency and effectiveness, the PCIE and ECIE annually compile these challenges into a short report. This compilation is useful to Congress and the rest of the oversight community in identifying possible Governmentwide projects that warrant high-level attention and review. The management challenges most frequently identified by OIGs are detailed in the following chart:

Agency	Information Technology Management & Security	Performance Management, Measurement, & Accountability	Financial Management & CFO Statements	Procurement & Grant Management	Human Capital & Staffing	Public Health & Safety	Physical Infrastructure	Service to the Public
1. AID	X	X	X	X	X			
2. USDA ¹	X		X	X		X	X	X
3. DOC	X	X	X	X				X
4. DOD	X		X	X	X	X	X	
5. DOEd	X	X	X	X	X			
6. DOE	X	X		X	X	X	X	
7. HHS	X	X	X	X		X	X	X
8. HUD	X	X	X	X	X			X
9. DOI	X	X	X	X		X	X	
10. DOJ	X	X	X	X	X	X	X	
11. DOL	X	X	X	X	X	X		X
12. State	X	X	X	X	X	X	X	
13. DOT	X	X	X	X	X	X	X	X
14. Treasury	X	X	X					
15. VA	X	X	X	X	X	X		X
16. EPA	X	X	X	X	X	X	X	
17. FEMA	X	X	X	X	X	X	X	X
18. FDIC	X	X	X	X	X		X	X
19. GSA	X	X		X	X	X	X	X
20. IRS	X	X	X		X		X	X
21. NASA	X		X	X		X	X	
22. NSF	X	X	X	X	X		X	
23. NRC	X	X	X	X	X	X		X
24. OPM	X	X	X		X			X
25. SBA	X	X	X	X	X			
26. SSA	X	X			X			X
TOTAL	26	23	23	22	20	15	15	14

¹. USDA's first Performance and Accountability Report, to be issued on February 1, 2003, will include USDA OIG's identified management challenges. The information provided herein is a draft as of August 9, 2002.

Following the issuance of "A Blueprint for New Beginnings: A Responsible Budget for America's Priorities," the President announced his Management Agenda in August 2001. This agenda is designed to coordinate agency efforts to "address the most apparent deficiencies and focus resources where the opportunity to improve performance is the greatest." The agenda's goal is to establish a more responsible and responsive Government that is citizen-centered, results-oriented, and market-based. The administration is focused on the following five Governmentwide initiatives.

- ❑ Expanded Electronic Government.
- ❑ Budget and Performance Integration.
- ❑ Improved Financial Performance.
- ❑ Strategic Management of Human Capital.
- ❑ Competitive Sourcing.

Clearly, the events of September 11 have moved the protection of our homeland to the top of everyone's list. This initiative includes securing the Nation's physical and information infrastructures as well as the ever-present concern for the public's health and safety.

The fact that the initiatives the President is focused on closely relate to the Government's most significant management challenges identified by the IG community is not a coincidence. The IG community will continue, as it has since 1978, to focus on good, responsible Government. The examples that follow are clear evidence of this commitment.

Protecting the Homeland

By the time the President established the Office of Homeland Security and the Homeland Security Council on October 8, 2001, many OIGs had already begun work on homeland security issues. The mission of the Office is to develop, coordinate, and implement a comprehensive national strategy to secure the United States from terrorist threats or attacks.

The Office, in consultation with the Homeland Security Council, is responsible for coordinating efforts to detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States. Defending against further terrorist attacks poses enormous physical security challenges because of the sheer number of potential terrorist targets and the wide variety of weapons that could be used. The need to develop vaccines to fight the spread of anthrax and deadly diseases such as smallpox, help States and communities train and equip police and firefighters, improve intelligence collection and sharing, expand patrols at our borders, strengthen the security of air travel, and use technology to track the arrivals and departures of visitors to the United States is immediate when basic rights and freedoms are threatened.

The following are selected examples of individual OIGs' attention to the threat against our homeland.

In light of the events of September 11, **EPA OIG** and the Senate Committee on Environmental and Public Works asked EPA to report its current and immediate action plans to protect the Nation's water systems from terrorist attack. In a November 19, 2001, memorandum to the IG, EPA reported that the Administrator had established a Water Protection Task Force with a staff working full time on implementing PDD 63 and other related activities.

EPA has expanded its work to include support for all water systems, both drinking water and wastewater. This is a major initiative with national impact that merits continued attention to ensure that planned activities are implemented, milestones are met, and issues are reported, addressed, and corrected as soon as possible.

The Federal Emergency Management Agency (**FEMA**) **OIG** plans to monitor FEMA's efforts to support the Office of Homeland Security and the Homeland Security Council as their roles and missions are further defined. The FEMA Director is a member of the Homeland Security Council, which also includes the Secretaries of the Treasury, Defense, Transportation, and HHS; the Attorney General; and the Directors of the FBI and Central Intelligence Agency.

FEMA's mission is to lead and support the Nation in preparing for, mitigating, responding to, and recovering from any destructive event, whether natural or caused by humans. FEMA expects to play a major role in supporting the Homeland Security Office and Council. FEMA supports the recently developed Homeland Security Roadmap and expects to continue its efforts in supporting first responders with planning, equipment, training, and exercises.

OIG also noted that FEMA's focus on State and local preparedness has taken on a new urgency following the events of September 11. FEMA must continue to place a high priority on developing State and local capabilities to respond to terrorist events and natural disasters. It is critical that State and local capabilities be relied upon whenever possible.

Another challenge for FEMA is devolving more responsibility to States for responding to and coping with disasters rather than routinely issuing disaster declarations—especially for small and medium-sized disasters. Over the past decade, the frequency of federally-declared disasters has almost doubled.

Instead of responding only to major disasters such as earthquakes and terrorist attacks, FEMA is regularly called upon to respond to events that are fairly predictable—such as snowstorms and repeated flooding in flood-prone areas. Both Congress and OMB have urged FEMA to develop improved criteria for disaster declarations. While FEMA has agreed that disaster criteria could be clarified, resistance from stakeholders—especially States—has impeded FEMA's efforts to reform the criteria. The criteria should recognize the financial capacity of States and include capability thresholds that States are expected to meet prior to a declaration.

Also, the criteria should include incentives to States to enhance capability. Pursuant to a proposal in the President's FY 2002 budget blueprint, FEMA plans to improve its disaster assistance criteria guidelines for determining when and under what conditions a presidential disaster declaration should be made.

A number of **HHS** **OIG** reviews have addressed concerns about HHS departmental vulnerabilities and the readiness of responders at all levels of government to protect public health in areas such as bioterrorism. OIG is assessing security controls at HHS laboratories and plans to conduct these assessments at other laboratories, including examining how these institutions are handling the USA Patriot Act of 2001 prohibition on access to select agents by restricted persons.

The September 11 attacks revealed the vulnerability of Department of the Interior (DOI) employees, visitors, infrastructure, and national monuments to terrorist actions. As a result, **DOI** **OIG** elevated the objective of ensuring the adequacy of DOI's contingency planning and preparedness for natural disasters and terrorist attacks to a critical management challenge.

As part of responding to this challenge, OIG completed a Comprehensive Assessment of DOI Law Enforcement, including a review of security and emergency preparedness within DOI, and made several recommendations to the Secretary. Both OIG and DOI are committed to providing maximum protection to DOI resources under all possible circumstances, and OIG is now determining where it can best apply its resources to maximize its contribution to protecting DOI and its visitors.

DOT **OIG** testified before congressional committees on OIG recommendations for deployment and maximum use of explosives detection equipment for screening checked baggage. In numerous

testimonies, DOT OIG has reported on its post-September 11 review of checked baggage screening, where it found air carriers were not maximizing the use of explosive detection machines and that 73 percent of the machines were not in continuous use as required by FAA.

The events of September 11 also heightened attention to other aspects of DOT OIG's work, including oversight of the Federal Commercial Drivers License (CDL) program to minimize fraud and abuse and prevent unqualified individuals from driving big rigs on the country's highways, as well as computer security to protect networks from disruption and address the vulnerability of DOT's computer systems to hackers.

Fraud in the testing and licensing of commercial drivers is a significant problem that has compromised highway safety and the Nation's security. Since 1998, criminal law enforcement investigations of the States' CDL programs have identified schemes in 15 States for obtaining CDLs through fraud. Under Federal reciprocity rules, a State must allow any person to operate a commercial vehicle if the driver has a CDL issued by another State. Thus, problems with CDL testing and licensing in one State may easily spread to others unless a strong national CDL program is in place.

The events of September 11 added security concerns that future terrorist actions could involve hazardous materials delivered by truck. One of DOT OIG's top priorities is to work closely with the Federal Motor Carrier Safety Administration to strengthen the national CDL program and improve its oversight review of the State CDL programs.

SSA OIG was instrumental in providing information and recommendations that Congress has used to craft antiterrorism legislation. Aside from playing a major investigative role, SSA OIG continues its audit efforts to inform Congress and SSA of the importance of limiting the use of the SSN. Audit work reiterates that SSA needs to strengthen its business processes to prevent future fraudulent activities that may make it easier for terrorists to integrate themselves into U.S. society.

Managing Information Technology and the Transition to Electronic Government

We live in an increasingly interconnected society, where the Internet has spawned tremendous improvements in efficiency and customer service. People use the telephone and Internet to get service 24 hours a day, 7 days a week. More than 60 percent of all Internet users interact with Government Web sites, and this number is expected to grow. The President's budget states that there are more than 31 million Federal Web pages on 22,000 Web sites.

The President's E-Government strategy paper notes that the primary goals for this initiative are to:

- Make it easy for citizens to obtain services and interact with the Federal Government.
- Improve Government's efficiency and effectiveness.
- Improve Government's responsiveness to citizens.

OIGs across the Government agree that electronic technology can be used efficiently and effectively to improve services to the American taxpayer. However, appropriate controls need to be in place to safeguard the sensitive data and critical systems of Government. Since the Federal Government is expected to spend more than \$50 billion in 2003 on E-Government issues, the IG community must play a vital role in overseeing the resources dedicated in this area.

The following are selected examples of individual OIGs' work in the information technology and E-Government arena.

TIGTA notes that modernization of IRS technology is crucial to implementing the new business vision of providing world-class service to taxpayers. Key goals, such as having 80 percent of tax returns filed electronically by 2007 and significantly improving levels of service in answering taxpayer questions, are contingent on developing new technology.

Furthermore, while the new technology evolves, existing operations must continue and improvements must be made to meet the needs of tax administration and demonstrate to taxpayers the IRS' commitment to better services. As a result, TIGTA has identified systems modernization as a major management challenge facing the IRS in FY 2002.

In FY 2001, TIGTA reported the following areas that pose potential barriers to the success of business systems modernization:

- ❑ Delays and cost overruns in delivering tangible benefits to taxpayers.
- ❑ Potential funding problems.
- ❑ Inconsistencies in implementing key systems development processes.
- ❑ The fact that business needs are not always well defined.
- ❑ Lack of clarity as to which systems development projects should be classified as modernization projects.

According to **OPM's OIG**, OPM worked on two major Governmentwide projects in FY 2001. The first, the Electronic Human Resources Integration (EHRI), should improve the efficiency of moving human resources data electronically between agencies and provide the basis for the envisioned move to an integrated human resources system for the Federal Government.

The second, the Retirement Systems Modernization (RSM), is related to the Human Resources Data Network (HRDN) in that it will use the electronic data gathered as part of the HRDN and is OPM's central strategy to meet its long-term customer service, business, and financial management goals for the retirement program.

For the RSM project, the OPM OIG provided limited oversight by attending project status meetings and several process validation sessions. The OIG participated as subject matter experts in validation sessions for the Trust Fund and Employee Withholding core processes. The objectives were to review the accuracy of the contractor's documented understanding of the core processes, provide input to correct any inaccuracies, and confirm the contractor's final documented understanding. The auditors also offered recommendations for improvements in several other project working sessions.

Auditors reviewed selected goals and measures in OPM's Performance and Accountability Report for FY 2001 that included the RSM effort. The review included the verification and validation of performance data and an evaluation of the effectiveness of related controls. OIG found controls over the performance measurement data were adequate and the reported results were reliable.

OIG staff met with OPM officials to determine whether OPM was addressing E-Government items in its FY 2003 agency performance plan and outlined a general model for OPM to consider. Also, OIG will be verifying and validating FY 2001 performance data relating to E-Government issues.

DOS OIG identified weaknesses in the Department's critical infrastructure protection program. OIG found that the Department's international outreach strategy is unnecessarily constrained and does little to encourage the development of preventive measures needed to enhance global critical infrastructure protection. OIG also found that the critical infrastructure protection plan provided a suitable framework for addressing minimum essential infrastructure. However, the plan falls short

because it does not address potential cyber-vulnerabilities in its foreign operations or in its interagency connections.

ED OIG is reviewing E-Government initiatives. Under GPEA, the executive agencies must move to E-Government by October 2003. The purpose of GPEA is not simply to replace paper transactions with electronic ones but to help agencies improve program operations, achieve cost savings, and develop adequate controls to prevent fraud, waste, and abuse.

Agencies were required to develop and submit to OMB by October 2000 a plan that provides for implementation of GPEA by October 2003. During FY 2001, OIG reviewed ED's first plan submission and advised the Department to identify specific milestones to ensure completion and compliance with GPEA.

As the DOL increases its reliance on E-Government to deliver services, benefits, and program administration, **DOL OIG** is increasing its audit coverage in this area. During FY 2001, DOL OIG audited mission-critical information systems that DOL depends on to monitor and analyze the Nation's labor market and economic activities, manage workforce services, and protect and compensate American workers. These audits revealed specific vulnerabilities in computer security and protection of assets, and OIG recommended improvements.

The **FCC OIG** focused attention on the FCC's Web sites to determine whether they were accessible to disabled users. FCC OIG found that the FCC has a proactive and effective Web accessibility program.

The **National Archives and Records Administration (NARA) OIG** noted that the growth of Web access and E-Government, the availability of electronic access under the Freedom of Information Act as amended by the Electronic Freedom of Information Act, and provisions of GPEA will further increase demands for online records and services. OIG points out that NARA must master the challenges of preserving electronic records in a way that makes them usable; that is, available in systems through which users can locate, retrieve, and read needed records.

Better Integration of Budget and Performance Results

In May 2001, GAO reported that most Federal managers are largely ignoring performance information when allocating resources. With the administration's focus on improving program results through the integration of budget and performance initiatives, it is critically important that agencies move toward tying their GPRA initiatives to their budgets.

GPRA established requirements for agencies to develop strategic plans and performance targets and to report annually on the progress toward achieving their goals. According to a recent GAO study, agencies have made some progress in linking expected performance and program activity funding. However, GAO stated that additional effort is needed to clearly describe the relationships among performance expectations, requested funding, and consumed resources. The IG community continues to consider performance management, measurement, and accountability a significant Government management challenge.

Last year the PCIE responded to a request from Chairman Dan Burton of the House Government Reform Committee on the OIGs' assessment of the most significant performance measures in their agencies' performance reports and the extent to which the data or information underlying the measures was valid and accurate. Many OIGs assess GPRA-related performance measures as a standard part of their work. In addition, the IG community has an active GPRA Coordination Committee to address the challenge of achieving GPRA's intent within the IG community and respective agencies.

We believe that the President's Management Agenda initiatives are a promising first step. However, the success of these initiatives can be achieved only through updated, integrated information systems. Agencies will need to invest in updating their financial and program information systems and ensure that these systems are developed and approved in accordance with standard system architecture platforms.

The following are selected examples of individual OIGs' work in the area of performance management and measurements.

During 2001, the **Federal Reserve Board (FRB) OIG** audited the Board's efforts to implement performance management principles consistent with GPRA requirements. OIG performed this audit to assess the status of FRB's implementation efforts and to evaluate the benefits of fully integrating GPRA concepts into FRB's planning and budgeting process. Overall, OIG found that more work needs to be done to achieve the Board's objective of voluntarily complying with GPRA.

OIG's recommendations were designed to enhance FRB's current planning and budgeting process by developing a performance management framework and by adopting key performance management characteristics such as the following:

- ❑ A longer range planning horizon with an FRB-wide planning focus.
- ❑ Specific performance indicators and measures.
- ❑ Expanded performance reports detailing the levels of achievement relative to the performance measures.

FRB management generally agreed with the intent of OIG's recommendations and plans to address them. FRB OIG plans to follow up on FRB's actions as part of its 2002 audit work.

FCA OIG conducted a performance budgeting audit, and management agreed to 14 actions to integrate performance with budget. As a result, FCA identified products and services for each of its components and made budgeting more uniform. FCA also drafted a policy to institutionalize performance budgeting, streamlined its time tracking system to simplify the tracking of product and service costs, and is currently performing a staffing study.

The **DOE OIG** examined DOE's FY 2000 Performance and Accountability Report and evaluated whether it generally complied with GPRA requirements. After assessing the specific measures in this report, OIG selected 10 performance measures that most closely paralleled the major management challenges facing DOE as documented in OIG's November 2000 report "Management Challenges in the Department of Energy."

OIG reported that DOE has made progress in implementing GPRA. For the past 3 years, it has issued a comprehensive Performance and Accountability Report with established goals designed to define the level of performance to be achieved by each program. In addition, DOE has worked to incorporate performance goals and objectives into its management contracts. However, OIG identified problems with the usefulness and completeness of the performance measures and the validity and accuracy of some of its reported results.

A **Nuclear Regulatory Commission (NRC) OIG** audit determined that at least 13 of 29 safety-related performance measures and results in the FY 1999 Performance Report were either invalid or unreliable. In addition, the Performance Report did not adequately describe why NRC failed to meet one performance goal.

These problems were caused by inadequate management controls for ensuring the validity and reliability of the performance measures. Specifically, NRC lacked formal procedures or policies for addressing data collection, reporting results, and assigning staff responsibilities.

Improving Financial Performance

The administration is aggressively seeking to improve the timeliness, usefulness, and reliability of financial information to enable sound decisionmaking and to safeguard the Government's assets. Since the enactment of key legislation during the 1990s to improve Federal financial management, OIGs have worked closely with Federal entities to address financial management and accounting system weaknesses.

As a result, 18 of 24 CFO agencies received unqualified or "clean" opinions on their FY 2001 financial statements. For FY 2001, DOJ and DOT joined 16 other departments and major agencies in receiving clean audit opinions on their financial statements. USDA and ED, along with the Agency for International Development (AID), also showed substantial improvement over previous years. Two agencies moved down from their clean opinion status in FY 2000, receiving a qualified opinion and a disclaimer in FY 2001.

Much more needs to be done to improve the quality, timeliness, and usefulness of financial information and to enhance financial information systems. In our last annual report to the President, we mentioned that, for some agencies, attaining a clean opinion is a fragile and somewhat artificial achievement because it results from extraordinary end-of-year efforts rather than a more constant real time financial management system operation.

The administration's emphasis on accelerating the reporting requirements over the next few years to eventually require an audited financial statement within 45 days after the end of the FY will be a challenge. The CFO and IG communities will be working together to address this emerging issue. Other critical areas include streamlining agency processes and/or upgrading financial information systems and identifying more than \$20 billion in erroneous benefit and assistance payments.

The OIGs considered financial management a continuing management challenge. One area in which the IG community identified a Governmentwide problem in financial management and provided recommendations was the Federal collection of non-tax-delinquent debt, which amounted to more than \$46 billion. Currently, the IG community and CFOs are also conducting a joint project to determine the extent of erroneous payments and identify ways to address this \$20 billion problem. OIGs are continuing to devote considerable resources not only by assessing these types of finance-related problems but also by offering their expertise in evaluating accounting operations and financial information systems.

The PCIE also took the lead in discussing best practices among IGs and CFOs related to the ongoing financial statement work. In a June 2001 report entitled "Best Practices Guide: Coordinating the Preparation and Audit of Federal Financial Statements," the PCIE reported on a number of best practices being used in agencies, including the following:

- Establishing key milestones in writing.
- Consulting with GAO and OMB, as appropriate, to ensure consistency of approach Governmentwide.
- Holding regular IG and CFO progress meetings.
- Performing interim test work whenever possible and bringing identified issues to the attention of agency management.

By working together on implementing these best practices, the IG and CFO communities can foster an environment that supports the purposes and objectives of the CFO Act and Government Management Reform Act.

The following are selected examples of individual OIGs' work on improving financial management within the Government.

While performing the annual audits of the FDIC's financial statements, the **FDIC OIG** and GAO successfully implemented continuous auditing techniques. This approach was designed to eliminate periods of high demand on audit teams and FDIC personnel that occur during the normal course of an audit.

Traditionally, during the financial statement audit, auditors perform testing in one or two test intervals using 6 to 12 months of supporting documentation. Thus, an extended period would exist between the time the transactions occurred and communication of test results to management.

To provide more timely results, the continuous audit approach allows transactions to be tested monthly. Through a centralized, automated sample process, auditors determine the sample sizes and extract samples from the general ledger or other databases. The auditors then request supporting documentation from FDIC personnel, complete testing, and share results.

The FDIC OIG also assessed the reasonableness of the cost-benefit analysis and the systems architecture vision prepared to plan the FDIC's future financial environment. In addition, OIG evaluated whether the project team was recommending the acquisition of a basic or enhanced financial management system and the adequacy of the underlying support for this recommendation.

Although OIG identified limitations in the cost-benefit analysis estimates, the need to modernize FDIC's financial management system suggested that it should proceed with acquisition planning for a commercial off-the-shelf financial management system. In response to OIG's recommendations to have more complete and accurate information before approving such a large technology investment, the FDIC Board of Directors approved the project but decided to establish funding and periodic reporting parameters that would impose external discipline on the process.

FDIC's periodic reports will address updated funding requirements, integrating and interfacing systems issues, reengineering business processes, acceptance testing, and other funding issues. FDIC OIG is continuing to monitor the agreed-upon corrective actions as the project evolves, and will conduct additional reviews during the various stages of the project.

One of the greatest management challenges confronting USDA is achieving financial accountability. For the past 6 years, **USDA OIG** has disclaimed an opinion on the Department's consolidated financial statements. This means the Department does not know whether it properly accounted for the money it collected, the cost of operations, and assets of well over \$100 billion.

Consequently, some USDA managers are forced to make decisions on program operations without solid financial data. The Department's problems with its financial management system will continue until at least 2003, at which point all USDA agencies should be converted to the Foundation Financial Information System (FFIS).

Effective implementation of FFIS is needed to improve the Department's financial management, thereby ensuring that managers have reliable data to manage their programs. At the same time, USDA OIG investigative work continues to confirm the vulnerability of USDA programs to general contract fraud and embezzlement, and has resulted in the recovery of millions of dollars.

FEMA OIG stated that FEMA faces a significant challenge in addressing longstanding financial management problems and garnering resources to correct them. FEMA does not have a functioning, integrated financial management system, and its system of internal controls has material weaknesses.

For years, these deficiencies have adversely affected FEMA's ability to record, process, summarize, and report accurate, reliable, and timely financial data and have increased the risk that material errors or irregularities could occur without detection.

Between FYs 1992 and 2001, FEMA successfully invested in its disaster preparedness, response, recovery, and mitigation programs. However, this investment was made at the expense of FEMA's infrastructure (i.e., human resource management, IT management, and financial management). Owing to resource constraints, policies and strategies for resolving financial management problems and enhancing financial operations were either ignored or limited to the most fundamental tasks.

As a result, FEMA's financial operations continue to deteriorate each year, creating an unstable financial management environment and jeopardizing FEMA's ability to fulfill its financial management responsibilities in future years. This situation is particularly troublesome in light of the increased responsibilities and associated funding that FEMA has received in response to the events of September 11.

To fulfill these important new responsibilities effectively and efficiently, FEMA must develop and maintain an enhanced financial management and internal control structure that includes an integrated accounting system and ensures reliable and timely financial reporting.

FEMA OIG has documented waste and mismanagement at grantee and subgrantee agencies throughout the country over the past 7 years. Between 1993 and 2000, OIG's audits of disaster assistance grants have questioned the use of funds totaling nearly \$900 million.

In addition, during the past 3 years, FEMA OIG completed audits in 17 States covering FEMA's management of disaster grants. There are a number of recurring grant management problems among the States. For example, States often do not monitor and accurately report on subgrantee performance and financial activities or make payments or close out projects in a timely manner, and financial status reports filed with FEMA are often incorrect or untimely.

States do not always maintain adequate documentation supporting their share of disaster costs and other financial requirements. Although FEMA has been very aggressive in correcting the problems FEMA OIG has reported, much can be done proactively to prevent such problems from recurring.

On the basis of a statistical sample, **HHS OIG** estimated that improper Medicare benefit payments made during FY 2000 totaled \$11.9 billion, or about 6.8 percent of the \$173.6 billion in processed fee-for-service payments reported by the Centers for Medicare and Medicaid Services (CMS). This error rate is slightly less than half that initially estimated by OIG in FY 1996, primarily because of CMS' corrective actions and work with the provider community to clarify reimbursement rules.

Causes of these improper payments could range from mistakes to fraud or abuse. Contractors claim that processing controls were not effective in detecting the kinds of errors the OIG audit found. While OIG's 5-year analysis indicated continuing progress in reducing improper payments, unsupported and medically unnecessary services remained pervasive problems, accounting for more than 70 percent of the total improper payments over the 5 years.

HHS OIG also found that some States inappropriately inflated the Federal share of Medicaid by billions of dollars by requiring public providers to return Medicaid payments to State governments through intergovernmental transfers. The States used the funds for other purposes, some of which

were unrelated to Medicaid. This practice was noted in two types of payments: Medicaid enhanced payments available under upper payment limits and Medicaid disproportionate share hospital payments.

HUD OIG's annual financial audits of the Department continue to report numerous problems related to inadequate system integration. For example, the lack of an automated interface between the departmental general ledger and the Federal Housing Administration (FHA) subsidiary ledger necessitates extensive manual analyses, reprocessing, and additional entries.

FHA's funds control process is also largely manual. Other serious deficiencies include the inability to identify, in a timely fashion, excess funds on expired Section 8 projects and inadequate assurance about the propriety of Section 8 rental assistance payments. As yet there is no systems solution to these problems.

DOT OIG noted that the development of a cost-accounting system is important because operating administrations such as the FAA, the Coast Guard, and the new Transportation Security Administration need good cost accounting information in order to improve operations and make informed management decisions.

FAA has made progress on its cost accounting system during the past year. However, problems with implementing Delphi—FAA's new financial system—are leading to delays in implementing cost accounting systems. DOT as a whole must have a credible cost accounting system to manage its programs, to know the real cost of services provided, and to identify areas where costs can be lowered without an adverse impact on service.

According to **DOD OIG**, the Secretary of Defense has established the Defense Financial Management Modernization Program to provide policy direction and central control for all DOD financial management improvement efforts. Led by the Under Secretary of Defense (Comptroller), this effort appears to be better structured and more comprehensive than the disjointed DOD efforts of the past several years. New emphasis on business process reengineering, providing useful financial information to managers, and reducing the number of systems processing financial data is encouraging and merits strong support.

DOD OIG is encouraged by the primary focus of OMB, Congress, and DOD on attaining financial management systems that facilitate more efficient operations. In prior reports and hearings, DOD OIG has expressed concern about the widespread preoccupation with clean audit opinions on end-of-year financial statements.

In the absence of adequate financial reporting systems, favorable audit opinions for virtually all major DOD financial statements were impossible, yet unrealistic goals continued to be set. To fulfill mandatory audit requirements, the DOD internal audit agencies were forced to apply disproportionate resources to financial statement audits. Not only was much of this effort repetitive, it also siphoned scarce audit resources away from other important areas.

For its FY 2000 consolidated financial statements, DOC received its second unqualified or clean opinion. However, maintaining a clean opinion on consolidated statements remains a major challenge, according to **DOC OIG**. Audits of the FY 2000 statements identified six material weaknesses (serious flaws in the design or operation of an internal control component that increase the risk of errors, fraud, or noncompliance), seven reportable conditions, and several instances of noncompliance with laws and regulations.

Managing Procurement and Competitive Sourcing

Across the Government, increased emphasis is being placed on outsourcing tasks that are readily available in the commercial marketplace, such as administrative support, certain aspects of facilities management, and payroll services. Historically, the Government has realized significant cost savings through competitive sourcing.

In November 2001 testimony, GAO noted that "Federal agencies spend billions of tax dollars each year to buy services, ranging from clerical support and consulting services to IT services, to the management and operation of Government facilities, such as national laboratories. And the amount spent on services is growing substantially. Last year alone, the Federal Government acquired more than \$87 billion in services—a 24 percent increase in real terms from FY 1990."

Again this year, the OIGs have identified procurement and grant management as a major management challenge. The Federal Government has been lax in its contractor oversight. Our annual reports to the President are full of examples of poor contractor oversight resulting in excessive and unnecessary costs to the taxpayer and, even more alarming, of fraudulent billing schemes.

OIG reports note that appropriate internal controls and oversight of these areas must be in place to ensure that goods and services not only meet the needs of the Government and the public but are provided in the most cost-effective and efficient manner. OIGs are continuing to look at how Federal departments and agencies have been facilitating contract completion and providing oversight of the contractors.

The following are selected examples of individual OIGs' work in managing procurement and competitive sourcing within the Government.

DOD is the world's largest purchaser of services, at a cost of well over \$50 billion annually. **DOD OIG** reports that DOD has taken commendable steps to provide more oversight of the largest contracts for services, but the thousands of other contracts and purchase actions for services remain a challenge. DOD OIG reported continued failure by DOD organizations to minimize sole source awards for task order contracts.

In addition, DOD OIG continued its series of audits on contracting for services by individual organizations and reported that a large DOD agency's contracting effort needed improvement. Congress has used these reports over the past year to change laws intended to improve the acquisition of services. DOD OIG reports also identified continued problems in purchasing supplies and spare parts, resulting from a combination of procurement personnel cuts, poorly designed purchasing systems, and inadequate oversight.

To restore credibility to the procurement process, DOD needs to make a more serious effort to avoid overpriced items, such as those identified this year to include \$409 sinks that should have cost \$39, \$2.10 screws worth \$.48, and \$.25 dust plugs worth \$.03. Although these unit prices may seem too low to warrant concern, the true picture emerges when we consider that DOD purchases tens of millions of such items annually.

DOT OIG found in a recently completed audit that DOT and FAA oversight of cost-reimbursable contracts totaling about \$4 billion annually is seriously inadequate. This vulnerability is particularly significant since FAA alone awarded some 800 cost-reimbursable contracts totaling \$3.4 billion in FY 2001. DOT OIG found that:

- ❑ FAA cost-reimbursable contracts totaling about \$2 billion did not have the required incurred-cost audits.

- ❑ About 1,800 contracts totaling around \$6 billion were completed for 3 to 12 years but were not closed timely.
- ❑ Contracting officers did not always have the documents to determine appropriate payments.
- ❑ Contract files frequently did not include evidence that contractors' accounting systems were adequate.

FAA's oversight of cost-reimbursable contracts is particularly inadequate. OIG paid for audits by the DCAA until 1996, when Congress transferred the financial responsibilities to DOT agencies. Completed audits for DOT dropped from 468 in FY 1995 to a low of 53 in FY 1997. At the direction of the House Transportation Appropriations Subcommittee in FY 2000, the number of audits has begun to rise and totaled 169 in FY 2001. Although independent audits are increasing, these high-risk, cost-reimbursable contracts need more audit scrutiny.

Last year, **HUD OIG** audits of FHA loan origination practices found significant problems with FHA's reviews of lender underwriting and property appraisals. Deficiencies included the oversight of pre-endorsement contractors and the accuracy of information in the automated system tracking property appraisals. Therefore, HUD's risk of losses from inflated appraisals, fraudulent underwriting, property flipping, and other lending abuses increased.

Fraud and abuse by nonprofit organizations in HUD Single Family Programs also appears to be pervasive. Recent OIG audits found that FHA was receiving little or no benefit from discounted sales of HUD-owned property to nonprofit organizations. Many organizations were either fronts for profit-motivated entities or were unduly influenced by real estate agents, consultants, investors, contractors, and lenders. Discounted sales should have reduced the ultimate costs to low- and moderate-income homebuyers.

In the area of HUD's Public and Assisted Housing Program administration, a recent study of rent determinations estimates that errors made by intermediaries result in subsidy overpayments of \$1.7 billion and underpayments of \$6 million annually. Payment errors of this magnitude take on added significance in light of HUD's estimate of 4.9 million unassisted households. These households pay more than half their income for housing or live in severely substandard housing. The reduction of subsidy overpayments is a top priority of this administration, and a task force is currently preparing a comprehensive plan for achieving these results.

After a **USDA OIG** investigation of a Philadelphia corporation, its president and vice president were indicted for contract fraud. The fraud involved a \$4.5 million renovation project at an Agricultural Research Service research station in Pennsylvania, as well as a \$1.1 million DOD renovation project. The corporation failed to pay subcontractors, resulting in construction delays. The president of the corporation pleaded guilty in July 2000. The president and vice president were incarcerated, and the officers and the corporation were ordered to pay nearly \$2 million in restitution.

The **NASA OIG** found that between FY 1993 and FY 2000, the percentage of NASA funding available for competition decreased from 81 percent to less than 56 percent of the total obligations available. The percentage of total annual NASA procurements that were sole source rose from 35 percent in FY 1999 to 37 percent in FY 2000. During FY 2001, OIG inspections reviewed five sole-source acquisitions at five different NASA centers. The reviews disclosed that the acquisitions were not adequately justified in accordance with the Federal Acquisition Regulation. As a result, at least three procurements were subsequently cancelled, and others are under review. An audit of multiple-award contracts at two NASA centers identified that almost 50 percent of the 104 sole-source orders reviewed did not provide for adequate competition. A series of audit reports also questioned sole-source subcontracting by prime contractors under NASA contracts. Improper sole-source subcontracting by prime contractors may increase costs to the Government.

GSA's Multiple Award Schedule contracting program has grown exponentially, with sales of \$13.6 billion in FY 2000. As the program has grown, **GSA's OIG** has been concerned that certain program fundamentals, which are set out by regulation to achieve competitive pricing, have been marginalized.

An OIG white paper revealed that GSA was not consistently negotiating volume pricing on photocopier and IT schedules because procurement officials were not leveraging the Government's aggregate buying power and often failed to properly evaluate differing terms and conditions. OIG also reported that only 2 percent of the \$199 million in recommended cost avoidances were sustained on recently awarded photocopier contracts. In addition, 50 percent of contract extensions reviewed were executed without meaningful or vigorous price analysis, and requests for pre-award audits decreased by almost 90 percent.

DOE OIG conducted an audit to determine whether cost savings anticipated from the use of fixed-price contracts for environmental cleanup activities will be realized. OIG found that projected savings associated with 9 of 11 contracts reviewed were not likely to be fully realized. Some savings estimates were unsupported. Some were based on invalid cost comparisons, and others were invalid because increases in actual costs had occurred or were likely.

ED OIG assessed the management of Government property by three ED contractors and identified similar internal control weaknesses at all three. The audits disclosed significant supervisory and procedural weaknesses in the management of Government property. OIG found that the contractors did not properly identify the property and did not comply with recordkeeping, reporting, or inventory requirements. OIG recommended several corrective actions, and all three contractors generally agreed with the findings.

DOC OIG finds that as DOC increases its reliance on contractor-provided goods and services, at a cost of more than \$1 billion annually, its efforts to monitor the effectiveness of the acquisition process grow as well. Several laws were enacted during the 1990s to improve and streamline procurement practices. However, GAO and OMB's Office of Federal Procurement Policy, along with the IG community, continue to report problems with implementation of reform initiatives.

DOC OIG identified a number of problems in this area, such as the following:

- ❑ Inadequate use of performance-based service contracting.
- ❑ Lack of security provisions in contracts for IT services.
- ❑ Improper use of task order contracts.
- ❑ Insufficient planning for contract administration and monitoring.
- ❑ Inadequate management of the purchase card program within DOC.

Strategic Management of Human Capital

In January 2001, GAO reported to Congress that strategic human capital management is a high-risk, Governmentwide issue needing immediate attention. According to GAO, more than half the Federal workforce—about 900,000 employees—will be eligible to retire by 2005. In addition, to ensure that Government's as well as citizens' needs are effectively, efficiently, and economically met, Federal agencies must restructure human capital strategies to meet future challenges.

The wave of expected retirements, recruitment and retention obstacles, inadequate evaluation and reward systems, and outdated training and education methods are areas that need immediate attention. The administration's goal is for each agency to develop a viable human resource strategy

to attract and retain the right people, in the right places, and at the right time to enable the agency to be a high-performance organization that delivers high-quality services to the American public.

Members of the IG community believe this area is a major management challenge, not only for their respective entities but also for each OIG. The theme of a recent issue of our *Journal of Public Inquiry* emphasized the challenges Government agencies and the IG community are facing with regard to human capital issues. This publication contained articles on the following topics:

- ❑ Evaluating the efficacy of agency human capital systems.
- ❑ Recruitment strategies to attain a high-quality, diverse workforce.
- ❑ Building an organization for higher performance.
- ❑ Succession planning and training needs.
- ❑ Telecommuting and offsite workplaces.

PCIE has also realigned its committee structure by establishing a Human Resources Committee to create and implement innovative and effective human resource management programs within the community. As the Federal Government transforms itself to meet the challenges of the 21st century, it needs to answer long-unresolved questions about the size and requisite skills of its workforce.

Although we support more flexible personnel management rules and procedures, those are merely tools with which to shape the workforce. The primary management emphasis should be on sound planning to resolve the basic goals for workforce size and skills.

The following are selected examples of individual OIGs' work in the human capital area.

DOD OIG has noted that DOD, like most Government organizations, faces a range of serious personnel management issues related to an aging workforce. Moreover, the deep cuts in both the military force structure and the civilian workforce after the end of the Cold War were not accompanied by proportionate reductions in the number of military force deployments or in civilian workload. On the contrary, military operating tempo has been very high, and there are indications of morale problems among both military and civilian personnel.

Among the negative effects of downsizing are increased retention problems because of slow promotions and overworked staffs, recruiting problems, and skills imbalances. A series of reports on acquisition, financial operations, and quality assurance have demonstrated the problems of inadequate numbers of personnel to perform functions.

For example, one DOD OIG audit found that a 27 percent reduction in acquisition personnel over 2 years at a DOD supply center resulted in a 26 percent increase in administrative lead time for buyers to acquire parts and supplies, a 48 percent increase in back orders, and a 40 percent increase in backlogged purchase requests. These results demonstrate the need for decisions on any additional workforce sizing to be underpinned by careful analysis of workload and realistic productivity projections.

DOS OIG reviews show that recruitment, retention, and professional training for Foreign Service and Civil Service employees are critical issues. Although the Department is beginning to develop the workforce planning needed, it has far to go. OIG found that inadequate training and support for first-tour consular officers has led to lapses in nonimmigrant visa management at some posts.

Because GSA has downsized its workforce by 30 percent in recent years, **GSA OIG** performed a benchmark review of how other Federal and private sector organizations assess progress in acquiring a workforce with the skills and talents needed to meet 21st-century demands. While many

parts of GSA had begun the process of ensuring an adequate workforce, OIG reported that GSA needs to establish a unified strategy to ensure that it has highly talented professionals to meet the challenges of the future.

OIG advised management of the actions taken by several Federal agencies in conducting their workforce self-assessments. The assessments not only demonstrate senior-level commitment but also map out, in an objective fashion, the agencies' human capital requirements to meet current and future demographic and performance challenges.

The **U.S. International Trade Commission OIG** conducted an inspection of the Commission's largest resource and its most significant management challenge—human capital. Because nearly one-third of the Commission's workforce is eligible for regular retirement by 2005, OIG suggested that the Commission address human capital in its strategic plan and develop formal workforce succession, recruiting, and hiring plans.

NSF OIG reported that NSF is vulnerable to a wave of retirements in key areas as 63 percent of its executive workforce, as well as a large percentage of its science and engineering staff, are eligible to retire within 5 years. Meanwhile, NSF's budget for salaries and expenses continues to lag behind the growth of its overall program budget.

According to **NRC OIG**, one of the most serious management challenges facing NRC is workforce planning to maintain a highly competent staff to carry out NRC's public health and safety mission. One aspect of workforce planning focuses on achieving labor continuity so that when employees leave, NRC has developed candidates to fill their positions. This is particularly important since about 15 percent of NRC's employees are eligible to retire within 5 years, and the percentage is 20 percent or greater in some technical offices.

Ultimately, workforce planning should provide managers with a framework for making staffing decisions on the basis of NRC's mission, strategic plan, budgetary resources, and desired workforce competencies. An OIG audit revealed that NRC is making a concerted effort to strengthen its workforce planning approach. However, it lacks a comprehensive, organizationwide workforce plan.

NRC OIG found that NRC had not yet fully integrated workforce planning into its budget process, communicated its approach throughout the Commission, or institutionalized its efforts in a holistic plan that coordinated the various efforts then under way. Until NRC develops and implements such a plan, the future of its workforce planning efforts is at risk.

TIGTA has identified human capital management as one of the major challenges facing IRS for FY 2002. IRS faces a range of serious personnel management issues, ranging from recruiting, training, and retaining employees to problems associated with its recent reorganization and modernization efforts. IRS has struggled with a continuing need to properly staff, train, and provide adequate tools for its employees.

In FY 2001, TIGTA reported the need for IRS to coordinate among its functional areas to implement an IRS-wide workforce planning model that would identify strategic workforce requirements and be used in developing the strategic plan and budget. TIGTA also identified other reorganization and human resource issues, including programs that did not have direct control over field employees in another IRS functional area.

AID OIG reports that recruitment and retention of technically proficient personnel presents a major challenge for AID management. To assist management in meeting this challenge, OIG plans to audit AID's foreign language training program and its succession planning efforts to address anticipated gaps in skills caused by upcoming worker retirements.

In addition, OIG will audit the quality of services provided by AID's Office of Payroll in light of the recent transfer of employee payment activity to the National Finance Center's payroll and personnel processing systems. Many employees had expressed high levels of dissatisfaction with AID's payroll operations immediately following the transfer of operations.

The **Federal Election Commission (FEC) OIG** completed a special project related to human capital management in early FY 2002. The project's objective was to compile and analyze data on the retirement eligibility and projections for FEC employees over the next 10 years. The data analysis included a comparison of the projected employee retirements for FEC and the Federal Government in the Washington, DC, area.

OIG's analysis resulted in a conclusion that the risk associated with losing substantial numbers of employees to retirement is considerably less for FEC than it is for the Federal Government as a whole. Based on October 2000 data, OPM predicted that by the end of 2006, 13.5 percent of FEC's staff will have retired, compared with 22.8 percent of Federal Government staff in the Washington, DC, area.

OPM predicts that by the end of 2010, 25.6 percent of FEC staff will have retired, compared with 38.7 percent of Federal Government staff in the Washington, DC, area. OIG found FEC's staff to be younger, with fewer years of service than the Washington, DC, Federal Government averages. Although OIG concluded that the overall staff retirement scenario appears to be reasonable for FEC, it suggested that management begin to incorporate goals addressing human resource strategies into future GPRA performance plans.

Watching Over Public Health and Safety

The Federal Government has an enormous role in protecting the health and safety of its citizens. Whether the issue is the food we eat, the roads we drive on, the airports we travel through, the hospitals we visit, or even the air we breathe, the Federal Government has a duty to ensure that appropriate standards are maintained to protect all Americans.

While Federal agencies have risen to this challenge, more needs to be done to ensure sufficient Federal implementation of relevant laws. As the White House noted in the overview to the FY 2003 budget:

"Federal programs are responsible for providing services that are critical to the people's welfare. The public deserves at least the same commitment to results from its government that it expects from businesses. We will know we are successful when conversations no longer focus on how much we are spending on a program compared to last year but rather how the results of the program will change. Will we feed more people per dollar, educate more children per dollar, conserve more land per dollar, and so on?"

The IG community believes public health and safety is a key function of Federal Government and poses many challenges for Federal leaders. Improving Government performance in this area is critical to the well-being of every citizen.

The following are selected examples of individual OIGs' work in the area of public health and safety.

With the outbreak of foot-and-mouth disease in Europe and, subsequently, South America, **USDA OIG** conducted a special expedited review of the controls and procedures employed by USDA to prevent the entry of the disease via imported meat. Auditors found that enhanced controls were needed to reduce the possibility of the disease entering the United States.

The review found that communications between the Animal and Plant Health Inspection Service (APHIS) and the Food Safety and Inspection Service (FSIS), the two USDA agencies responsible for regulating the entry of imported meat, were weak. APHIS needed to improve its accountability over imported products from their arrival at U.S. ports of entry through their disposition by the respective agencies. APHIS and FSIS agreed with the findings and recommendations and are acting on them.

Three USDA OIG investigations to pursue specific threats resulted in significant criminal penalties against meat processors that distributed products contaminated by the deadly bacteria *Listeria monocytogenes*, which had sickened and killed people who consumed it. The USDA's rapid emergency responses immediately halted distribution of the products.

In one June 2001 case, attorneys for a major food-processing corporation pleaded guilty in U.S. District Court to producing and distributing adulterated meat and poultry products. From June to September 1998, one of its processing plants produced and distributed food products that contained *Listeria monocytogenes*.

Sentencing included the maximum fine of \$200,000 with an agreement to underwrite food safety research projects by funding a \$3 million grant to Michigan State University. The corporation also settled a civil lawsuit relating to the 1998 sale of meat products to DOD by paying \$915,800, as well as Government investigative costs, resulting in a total civil settlement of more than \$1.2 million.

A **DOE OIG** review of DOE activities involving biological select agents revealed a lack of sufficient Federal oversight, consistent policy, and standardized implementing procedures, resulting in the potential for greater risk to workers and possibly others from exposure to biological select agents and select agent materials that DOE maintains.

DOE OIG discovered questionable contract implementation and administration at a DOE site that resulted in serious environmental, safety, and health concerns. Examples included the mishandling of radioactively contaminated equipment, the presence of a number of fire and electrical hazards, and the leakage of possibly hazardous substances from equipment. The State of Ohio subsequently fined the contractor for nuclear safety violations.

The **EPA OIG** reports that the quality and integrity of laboratory data supplied to EPA for regulatory compliance, enforcement, policy, and remediation purposes continues to be a pressing issue. Environmental data of questionable authenticity can lead to concerns about the soundness of EPA decisions pertaining to the protection of the environment and public health. Furthermore, data integrity issues lead to additional costs and unnecessary delays when EPA has to identify and assess the impact of the fraudulent data and undertake additional sampling.

EPA OIG reviews and investigations have disclosed a particularly disturbing trend in the number of environmental laboratories that are providing misleading and fraudulent data to the States for monitoring the Nation's public water supplies and other indicators of health hazards, such as air toxins, pesticides in food supplies, and hazardous wastes.

A **DOJ OIG** review found that INS is placing the traveling public at potential risk because it does not consistently follow its established escort policy. To protect the traveling public, INS in 1998 adopted a policy of assigning INS officers to escort potentially dangerous aliens who are being removed from the United States on commercial flights. In three of the four districts OIG visited, INS managers disregarded this policy. OIG also found that INS often failed to provide the required ratio of escorts to dangerous aliens, and that INS did not always provide escorts during the final segment of multiflight removal trips. In addition, OIG found that INS does not adequately coordinate the alien escort process with DOS.

Tennessee Valley Authority (TVA) OIG notes that as an environmental steward and the Nation's largest public power provider, TVA strives to balance business requirements with environmental protection. TVA's environmental responsibility includes compliance with both Federal and State regulations. Air quality, watershed management, and other environmental issues, such as the presence of polychlorinated biphenyls (PCB), have warranted TVA's attention in recent years. Air quality issues have recently drawn the most public attention and could have the most profound economic effect as TVA seeks to provide cost-effective measures to achieve environmental compliance.

TVA OIG monitors environmental issues and includes significant items in its monthly emerging issues newsletter. It also participates in an Environmental Crimes Joint Task Force on an ongoing basis. During FY 2001, TVA OIG cosponsored an environmental training course for auditors at TVA, began an audit of TVA's compliance with Section 6002 of the Resource Conservation and Recovery Act, and, as a result of prior audit work, assisted a TVA team dealing with PCB abatement issues at TVA's request. Planned audit coverage in FY 2002 includes a review of TVA's environmental audit function for compliance with applicable auditing standards.

Safeguarding the Nation's Physical Infrastructures

The events of September 11 highlighted the importance of protecting the Nation's critical information infrastructures, which are essential to the operations of the economy and government. Because of the Federal Government's major responsibilities for public health and safety, dramatic and widespread harm would result should its systems be compromised. These systems include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both government and private.

Many of the Nation's critical infrastructures historically have been physically and logically separate systems that had little interdependence. However, as a result of IT advances and improved efficiency, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and cyber-attacks. Addressing these vulnerabilities will require flexible, evolutionary approaches that span both the public and private sectors and protect both domestic and international security.

OIGs continue to view physical and information infrastructure as a major management challenge. Currently, we are continuing to assess the Government's IT risks through the review of its effort to protect physical and cyber-based systems under the Homeland Security Plan.

We are also conducting annual independent evaluations of the agencies' information security programs and practices as part of GISRA. It codifies existing OMB security policies and reiterates security responsibilities outlined in the Computer Security Act of 1987, the Paperwork Reduction Act, and the Clinger-Cohen Act of 1996. In addition, GISRA requires annual agency program reviews and annual independent evaluations for both unclassified and national security programs. Our IT Roundtable is working with OIGs to address GISRA requirements through forums and training sessions with groups such as the CIO Council, OMB, GAO, and other organizations.

In March 2001, PCIE and ECIE presented the results of Phase I of a four-phase review of Federal agencies' implementation of PDD 63 related to critical infrastructure protection. PDD 63 called for a national effort to ensure the security of the Nation's critical infrastructures, "those physical and cyber-based systems essential to the minimum operations of the economy and government."

Overall, the OIGs' report stated that the Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. Specifically, the review found that many agency plans were incomplete, most agencies had not identified their mission-essential

infrastructure assets, and almost none of the agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

When all participating OIGs complete their Phase I reviews, they will have an estimated 100 recommendations to improve their respective agencies' critical infrastructure plans.

The following are selected examples of individual OIGs' work in safeguarding the Nation's physical infrastructure.

In its GISRA review, **USDA OIG** disclosed that USDA is still far from effectively managing and securing IT resources. Audits have identified that USDA, through the work of the Office of the CIO, has a departmentwide security plan in place and has begun improving the security of its IT resources. Despite its efforts, however, USDA remains noncompliant with several OMB Circular A-130, *Management of Federal Information Resources*, and PDD 63 requirements.

Before the appointment of a CIO, departmental agencies and staff offices addressed their respective IT security and infrastructure needs separately. These isolated approaches have resulted in a disparate array of technical and physical solutions that do not always ensure comprehensive departmentwide security.

USDA OIG is also accelerating a review of controls over accidental or intentional release of biohazards. The review emphasizes pathogen accountability and personnel and physical security of USDA laboratories around the Nation where the Department stores biological materials (used in research and diagnostic work) that could be harmful to plants and animals.

USDA OIG also reported that numerous program participants were convicted for illegally gaining millions of program dollars via electronic commerce systems such as the Food Stamp Program's Electronic Benefits Transfer system.

DOD OIG reports that DOD information systems are probed daily and are often attacked systematically by vandals, curiosity seekers, and other individuals with more sinister motives. Security is a major challenge to operators and users of all networked information systems. DOD's concerns about security extend not only to its own systems, but also far beyond to the networks used to support the private sector infrastructures that sustain our military forces at home and abroad.

FCC OIG concluded its first evaluation under GISRA. OIG determined that FCC has a generally effective information security program, with acceptable practices for managing and safeguarding its technology assets. FCC recognizes that some areas in its information security management and operational and technical controls need improvement.

FEMA OIG reported that IT is vital to its ability to accomplish its mission, but it presents several management challenges. Increasing connectivity between systems, especially through the Internet, and constantly changing and evolving technology and communications create new opportunities for enhancing existing processes but also dramatically increase technology and security risks. As a result, FEMA must remain vigilant in guarding its systems and data.

In several audit reports, OIG recommended ways to improve FEMA's information security processes and controls. However, it has been difficult for FEMA to obtain sufficient resources to take corrective action.

The **Federal Trade Commission (FTC) OIG** reviewed controls over the release of information stored on the hard drives of "surplused" computers donated to charitable institutions and school districts. OIG found that 40 percent of the hard drives sampled from computers ready for release

outside FTC had not been scrubbed properly or had been scrubbed using an older, less effective erasure software, leaving password files and case-specific (and confidential) files such as subpoenas.

Given the vulnerability and expense of the surplus donation program, OIG recommended that management destroy hard drives before donating the computers rather than erasing and reinstalling the hard drives. With the money saved, FTC could install new drives purchased in bulk.

HHS OIG noted that HHS has made much progress in securing its most critical assets. However, recent OIG assessments found numerous weaknesses in entitywide security, access controls, service continuity, and segregation of duties. These weaknesses leave HHS vulnerable to:

- Unauthorized access to and disclosure of sensitive information.
- Malicious changes that could interrupt data processing or destroy data files.
- Improper payments.
- Disruption of critical operations.

The **Federal Labor Relations Authority (FLRA) OIG's** FY 2001 audit of FLRA's computer information security and a related follow-up evaluation by an independent contractor revealed substantial weaknesses in FLRA's information resource program and a lack of sufficient management attention to the growing automation needs of customers and Federal employees. As a result of the audit, FLRA management placed a long-needed focus on information resources and security to enable FLRA to keep up with the expanding requirements of E-Government.

DOJ OIG audits have disclosed serious problems in computer security that could lead to the compromise of sensitive systems and data. In FY 2001, DOJ OIG tested the effectiveness of information security control techniques for nine DOJ systems at the Executive Office for U.S. Attorneys, Federal Bureau of Prisons, Drug Enforcement Administration, Justice Management Division, and FBI. These systems included five sensitive but unclassified (SBU) and four classified systems.

In the five SBU systems, OIG found weaknesses in management, operational, and technical controls, including password management, logon management, user and account rights assignment, file and system configuration, and system auditing management. In the four classified systems, OIG found that select computer security controls were not implemented to protect the systems from unauthorized use, loss, or modification.

Penetration testing on three classified systems resulted in auditors obtaining access to the systems. Weaknesses found in the SBU systems are considered a low-to-moderate risk. Weaknesses in the classified systems, when considered collectively, are a moderate-to-high risk. Weaknesses were more extensive and material for the classified systems because they had not been subject to such frequent external reviews as the SBU systems.

DOJ OIG continues to identify mission-critical computer systems that were poorly planned, experienced long delays in implementation, or did not provide timely, useful, or reliable data. One such system is INS' Automated I-94 System, developed as an automated entry/exit system for use at land, sea, and air ports of entry to identify and track individuals when they enter and exit the country.

A 2001 DOJ OIG audit assessed the design and implementation of the Automated I-94 System and determined that INS has not properly managed the project. As a result, despite having spent \$31.2 million on the system from FY 1996 to FY 2000, INS did not have clear evidence that the

system met its intended goals, had gained the cooperation of only two airlines and was operating the system at only four airports, and was in the process of modifying the system. INS has since determined that the system will not meet the new requirements that Congress has set, and has terminated the program.

NSF OIG reports that NSF faces the challenging task of facilitating an open research culture while protecting its critical information assets against unauthorized intrusion. Although NSF has enhanced its security program by establishing an intrusion detection service and appointing a security officer, continuing efforts are needed to improve system security. OIG's review of NSF's information security program indicates that there may be weaknesses that increase security risks. NSF concurred with the recommendations and has initiated corrective action.

Recognizing the importance of system security a year ago, the **Corporation for Public Broadcasting (CPB) OIG** staff agreed to start a joint project with CPB's Office of Finance and Administration to address the security needs of its information systems. The effort resulted in identifying three major weaknesses in CPB automated systems.

CPB took several corrective actions to strengthen the safeguards of its data and records. CPB installed new antivirus software on its servers and implemented virus filtering on its e-mail system. Information systems are now protected by a multilayer firewall, and operating systems were improved to better protect CPB information. CPB and its OIG are currently working on procedures to prevent and handle threats.

In FY 2001, **SSA OIG** performed a number of audits and reviews in this area as required by GISRA. OIG's review determined that SSA is in substantial compliance with GISRA but needs to improve its protection of sensitive information in the areas of technical standards implementation and system security monitoring.

A review of SSA's Computer Security Program's compliance with applicable laws and regulations found that SSA lacked a strong framework for overall security administration, policy development, and policy implementation. OIG recommended that SSA restructure its security management hierarchy to heighten accountability.

SSA OIG audited employees' access to the Earnings Record Maintenance System (ERMS) and discovered that certain employees had access to ERMS above what was necessary to perform their duties. OIG also reviewed SSA's system to prevent and detect direct deposit fraud and found weaknesses in this system. OIG noted weakness in system policy, configuration, and monitoring of SSA's intelligent workstations/local area network.

During FY 2001, SSA OIG performed several reviews that analyzed the physical security of SSA's facilities and assets. First, OIG reviewed SSA's Critical Infrastructure Protection Program as it related to physical security and determined that updates to the Critical Information Protection Plan are needed. The needs include updating plans for performing its reviews of existing physical security policies and procedures, developing training goals to ensure that it has the personnel and skills necessary to implement a sound infrastructure protection program, and identifying SSA's interdependencies with other Federal agencies for its physical assets.

As part of SSA's FY 2000 and 2001 financial statement audits, SSA OIG reviewed SSA's physical security. OIG found a lack of enforcement of security policies for physical access to information resources at nonheadquarters locations such as SSA's regional offices, program services centers, and select Disability Determination Services. It also found that SSA needs to complete its Continuity of Operations Plan and update its Disaster Recovery Plan.

DOI OIG notes that DOI has not resolved its longstanding problems with computer security and overall system effectiveness. Chairman Steve Horn's House Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, in its annual assessments of agency information system security, has consistently ranked DOI near the bottom of the list. DOI's failure to maintain systems to properly account for Indian trust assets is well known.

DOI OIG reported computer security as a material weakness in FY 2000 and 2001. The first annual OIG review of DOI's IT security systems under GISRA found inadequate or nonexistent security plans and risk assessments as well as employees who were poorly trained in their security responsibilities.

OIG's report in DOI's Annual Report for FY 2001 again identified material weaknesses in DOI's financial management systems. Although on September 20, 2001, DOI's CIO issued an IT security plan establishing minimum standards for secure operations, the plan did not specify the steps needed to meet these standards and is not expected to be fully implemented until FY 2006.

A **Treasury OIG** audit of the U.S. Customs Service (Customs) electronic data processing controls identified one material weakness and three reportable conditions. The material weakness is that Customs still does not have an adequate disaster recovery capability. Customs has measures under way to eventually provide the needed improvements.

However, until these improvements are made, Customs' law enforcement and revenue collection operations remain vulnerable to disruption. The lack of adequate disaster recovery capability at Customs was the subject of a "7-day" letter issued by the Treasury IG to the Secretary of the Treasury in May 2000.

During FY 2001, the **Securities and Exchange Commission (SEC) OIG** performed several reviews relating to IT management and security, including general computer controls at headquarters and the regions, staff and contractor background investigations, controls over intranet Web site content, IT capital decisionmaking, operational risks in the Office of Information Technology, and information security program and practices (under GISRA).

The reviews identified many significant improvements and accomplishments of SEC relating to IT. OIG also made a number of recommendations to improve IT practices and procedures and to ensure compliance with relevant statutes and regulations.

A **VA OIG** report found information security weaknesses in VA systems. As a result, information security is designated a material weakness area under the Federal Managers' Financial Integrity Act. VA systems continue to be vulnerable to unauthorized access and misuse of sensitive information and data.

VA has started efforts to correct these weaknesses and work toward compliance with GISRA. However, the recently completed GISRA audit identified significant information security vulnerabilities that continue to place VA at risk.

Collaborative Efforts to Fight Fraud, Waste, and Abuse

During FY 2001, members of the IG community collaborated with one another and with other organizations and agencies to combat fraud, waste, and abuse in the Federal Government—with special focus on systems security, improper payments, and health care fraud. After September 11, this collaborative spirit was also called upon to fight terrorism. Highlighted below are some instances of successful collaborations within the IG community.

Conducting Operation Green Quest

Special agents nationwide, including those in the USDA OIG, are assigned to criminal investigative efforts and multiagency counterterrorism and financial task forces involved in Operation Green Quest. The purpose of this operation, which was announced by President Bush, is to identify and track possible sources of funding for terrorism. OIG efforts are focused on investigations of benefits trafficking to determine whether money is finding its way overseas. USDA OIG is tracing Government funds to determine whether they are being used to finance terrorism.

Conducting Operation Safe Travel

SSA OIG, Customs, DOT OIG, and Salt Lake City Airport staff came together with the U.S. Attorney's Office to investigate security issues related to the Winter Olympics under Operation Safe Travel - Salt Lake City, Utah. The operation originated when an airport supervisor expressed the belief that a large number of employees might have provided false SSNs to gain employment at the airport. Salt Lake City Airport management gave SSA OIG the names of approximately 600 contractors working at the airport. Customs was also given a list of employees with access to Customs secure areas.

Subsequent examination of wage information by SSA OIG for those employers revealed numerous earnings posted to incorrect SSNs. The U.S. Attorney's Office brought in Utah Homeland Security, which researched criminal histories on about 1,350 individuals who were working in highly secure areas of the airport. As a result, 69 individuals were indicted—including 61 for SSN misuse. Eight others were indicted on immigration-related charges or false statements on FAA employment certifications.

Improving Export Controls

OIGs for DOE, DOD, Treasury, DOC, and DOS conducted a joint review to determine the effectiveness of export controls for the transfer of sensitive materials and technology to countries of concern under the provisions of the National Defense Authorization Act of 2000. The objective of the review was to assess the policies and procedures for developing, maintaining, and revising the Commerce Control List and the U.S. Munitions List.

These reviews have substantially contributed toward improving the dual-use and munitions export licensing processes and have provided Congress with an objective and thorough analysis of these processes. The interagency export control reports provided timely and useful input to the congressional and executive branch efforts to reform the Nation's export controls.

Focusing on Electronic Crimes and Computer Security

USPS OIG, the Texas Department of Public Safety, the Royal Canadian Mounted Police, and the Canadian National Investigative Service joined forces to investigate a November 1999 attack on a USPS Web site. The investigation involved a hacking group known as "hv2k." As a result of the investigation, a Texas man is serving a 2-year sentence following his January 2001 conviction for breaching computer security and aggregated theft. A second hacker responsible for the intrusion was placed in pretrial diversion by the court.

The New York Electronic Crimes Task Force—which includes GSA OIG, the U.S. Secret Service, DOD, DOJ, the New York City Police Department, and representatives from the telecommunications industry—investigates telecommunications fraud (primarily involving Federal facilities in the New York metropolitan area). The task force is pursuing individuals who are committing fraud through the use of stolen Government calling card numbers, cloned cellular telephones, and electronic attacks on Government telephone systems. This cooperative effort was initiated when it was determined that such fraud was resulting in the denial of communication services to Government

agencies. During FY 2001, approximately 18 investigations were performed and 19 individuals were charged with related crimes, resulting in 11 convictions or pleas.

In cooperation with the FBI, NASA OIG arrested a hacker who had broken into computers at NASA and other Government institutions and had used stolen credit card information to purchase electronic equipment. The hacker was incarcerated for 21 months and ordered to pay \$87,736 in restitution.

Pursuing Education Grant Funds Fraud

Hermandad Mexicana Nacional Legal Center (HMNLC)—a California community-based organization—was indicted on three counts of false statements and three counts of mail fraud after a joint ED OIG, FBI, and FEMA OIG investigation. The investigation determined that HMNLC had significantly misrepresented the number of hours students attended, as well as the amount of program-related expenditures.

For the 3 fiscal years beginning in July 1995 and ending in June 1998, HMNLC received grant funds of approximately \$6.6 million to provide adult education courses, of which approximately \$3.2 million allegedly was not used for program-related expenditures.

Investigating Organized Crime and Labor Racketeering

DOL OIG has a unique program responsibility for investigating labor racketeering and organized crime influence or control in unions and the workplace. Specifically, DOL OIG identifies and curtails labor racketeering and corruption in employee benefit plans, labor-management relations, and internal union affairs. DOL OIG continues its collaboration with DOT OIG to investigate organized crime influence and labor racketeering in federally-financed highway and public infrastructure projects. The transportation industry received \$200 billion in funding over a 5-year period via the 1998 Transportation Equity Act, providing significant stimulus to transportation construction and maintenance.

Since some of the same corrupt contractors who engage in labor racketeering also defraud federally-awarded contracts in this sector of the public construction industry, DOT OIG asked DOL OIG to participate in the antifraud effort.

Targeting Credit Card Fraud

The Federal Government procurement process has become more dependent on the use of charge cards through the GSA SmartPay program. As a result, GSA OIG developed a national proactive effort targeting fraud and abuse of charge cards by Federal employees and others.

This effort resulted in 59 investigations in FY 2001. The cases—worked cooperatively with the U.S. Secret Service, DOC OIG, NASA OIG, the Federal Protective Service, and HHS—have resulted in 16 criminal convictions and 8 administrative actions.

Uniting to Reduce Health Care Fraud

In the 5 years that the Health Care Fraud and Abuse Control Program has been in place to combat health care fraud, coordinated efforts between the U.S. Attorney General and HHS OIG have yielded impressive results. More than \$3 billion has been returned to the Medicare Trust Fund and the Federal Government as a whole. More than 15,000 individuals and entities have been excluded from participating in federally-sponsored health care programs.

Cost savings attributable to recommendations to correct systemic vulnerabilities and improve program economy and efficiency are averaging more than \$11 billion per year. A centralized Healthcare Integrity and Protection Data Bank is up and running, and industry guidance and beneficiary outreach have been greatly expanded.

In FY 2001, these collaborative efforts resulted in the successful conclusion of the largest government fraud settlement ever reached. The largest for-profit hospital chain in the country (Healthcare Corporation HCA) agreed to plead guilty to criminal conduct and paid the Federal Government and several States more than \$840 million in criminal fines and civil penalties related to five areas of Medicare and Medicaid fraud. Contributing to this investigation and settlement were DOJ; the FBI; OIGs for HHS, DOD, VA, and OPM; and State Medicaid fraud control units.

TVA OIG continued to support health care fraud task forces and working groups sponsored by U.S. Attorney's offices in Tennessee. One earlier investigation resulted in a physician's guilty plea in FY 2001 and a sentence of over \$200,000 in restitution, prison time, supervised probation, and community service. This investigation was conducted by TVA OIG special agents, DOD, DOL, and investigators from Blue Cross/Blue Shield of Tennessee's Special Investigations Unit.

Partnering to Enforce Court-Ordered Child Support

In FY 2001, HHS OIG continued to make the detection, investigation, and prosecution of noncustodial parents who fail to pay court-ordered child support a priority. Working with HHS' Office of Child Support Enforcement (OCSE), DOJ, and other Federal, State, and local partners, HHS OIG developed joint programmatic and operational procedures to expedite the collection of child support and bring to justice those who willfully disregard their obligations.

From FY 1995 through FY 2001, HHS OIG opened 1,519 child support investigations nationwide, resulting in 456 convictions and court-ordered criminal restitution and settlements of over \$25.9 million. These results are attributable in large part to the effectiveness of shared resources and efforts in the law enforcement community.

One specific way in which HHS OIG approaches child support enforcement collaboratively is its participation with OCSE in six multiagency and -jurisdictional task forces. Through the coordination of law enforcement, criminal justice, and child support office resources, the task forces identify, investigate, and prosecute the most egregious criminal nonsupport matters at both the State and Federal levels.

By working together and sharing information, the task forces create a mechanism for communication and coordination through which stronger cases are identified and more cases are brought to successful resolution. The six task forces established as of FY 2001 collectively cover 29 States, the District of Columbia, and Puerto Rico.

PCIE Membership Addresses and Hotline Numbers

Mark W. Everson, Chair, PCIE Deputy Director for Management
Office of Management and Budget
17th and Pennsylvania Ave., NW
Room 350, Eisenhower EOB
Washington, DC 20503
☎202-395-5963

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
20th and C Street, NW, Mail Stop 300
Washington, DC 20551
☎800-827-3340 or 202-452-6400

Linda Springer, Controller-Nominee*
Office of Management and Budget
725 17th Street, NW
Room 9013, New EOB
Washington, DC 20503
☎202-395-9161

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

Joyce N. Fleischman, Acting 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

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

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

J. Russell George, Inspector General
Corporation for National and Community Service
1201 New York Ave., NW, Suite 830
Washington, DC 20525
☎800-452-8210

Joseph E. Schmitz, Inspector General
Department of Defense
400 Army Navy Drive
Arlington, VA 22202-2884
☎800-424-9098 or 703-604-8546

John P. Higgins, Jr., Acting 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

*Also members of the ECIE

1000 Independence Ave., SW
Washington, DC 20585
☎800-541-1625 or 202-586-4073

Nikki L. Tinsley, Inspector General
Environmental Protection Agency
401 M Street, SW
Washington, DC 20460
☎888-565-8740

Grant D. Ashley, Assistant Director*
Criminal Investigative Division
Federal Bureau of Investigation
935 Pennsylvania Ave., NW, Room 5012
Washington, DC 20535
☎202-324-4260

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

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

Amy L. Comstock, Director*
Office of Government ethics
1201 New York Avenue, NW, Suite 500
Washington, DC 20005-3917
☎202-208-8022

Janet Rehnquist, Inspector General
Department of Health & Human Services
330 Independence Ave., SW
Washington, DC 20201
☎800-447-8477

Kenneth M. Donohue, 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

Glenn Fine, Inspector General
Department of Justice
950 Pennsylvania Ave., NW, Room 4706
Washington, DC 20530
☎800-869-4499

Gordon S. Heddell, Inspector General
Department of Labor
200 Constitution Ave., NW, Room S-1303
Washington, DC 20210
☎800-347-3756 or 202-693-6999

Robert W. Cobb, Inspector General
National Aeronautics & Space Admin.
300 E Street, SW, Code W, Room 8V79
Washington, DC 20546
☎800-424-9183

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

Dan Blair, Deputy Director*
Office of Personnel Management
1900 E Street, NW

Washington, DC 20415-0001
☎202-606-1001

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
☎Health Care 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

Clark Kent Ervin, Inspector General
Department of State and the Broadcasting Board of Governors
2201 C Street, NW, Room 6817
Washington, DC 20520-6817
☎202-647-9450 or 800-409-9926

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
1500 Pennsylvania Ave., NW
Washington, DC 20220
☎800-359-3898

Pam Gardiner, Acting Inspector General
Treasury Inspector General for Tax Administration
1125 15th St., NW, Suite 700A
Washington, DC 20005
☎800-366-4484

G. Donald Hickman, Acting Inspector General
Tennessee Valley Authority
400 W. Summit Hill Drive
Knoxville, TN 37902-1499
☎800-323-3835

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

ECIE Membership Addresses and Hotline Numbers

Mark W. Everson, Chair, ECIE
Deputy Director for Management
Office of Management and Budget
17th and Pennsylvania Ave., NW
Room 350, Eisenhower EOB
Washington, DC 20503
☎202-395-5963

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

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

Clifford H. Jennings, Inspector
General
Appalachian Regional Commission
1666 Connecticut Ave., NW, Suite 215
Washington, DC 20009-1068
☎800-532-4611 or 202-884-7667

A. 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
401 Ninth St., NW
Washington, DC 20004
☎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

Stephen G. Smith, Inspector General
Farm Credit Administration
1501 Farm Credit Drive
McLean, VA 22102
☎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
Washington, DC 20424
☎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
☎202-326-2581

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

Len Koczur, Acting Inspector General
Legal Services Corporation
750 First Street, NE, 11th Floor
Washington, DC 20002-4250
☎800-678-8868 or 202-336-8936

Paul Brachfeld, Inspector General
National Archives and Records
Administration
8601 Adelphi Road
College Park, MD 20740
☎800-786-2551 or 301-837-3000

Herbert Yolles, Inspector General
National Credit Union Admin.
1775 Duke Street
Alexandria, VA 22314-3428
☎800-778-4806 or 703-518-6357

Daniel L. Shaw, Inspector General
National Endowment for the Arts
1100 Pennsylvania Ave., NW
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
4201 Wilson Boulevard, Room 1135
Arlington, VA 22230
☎800-428-2189

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

Deborah Stover-Springer, Acting
Inspector General
Pension Benefit Guaranty
Corporation
1200 K Street, NW
Washington, DC 20005
☎800-400-7242 or 202-326-4030

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
Victor Bldg., Suite 4200
750 Ninth St., NW
Washington, DC 20560
☎202-275-1671

Kenneth F. Clarke, Inspector General
U.S. International Trade Commission
500 E Street, SW, Room 515
Washington, DC 20436
☎800-500-0333 or 202-205-2210

Karla W. Corcoran, Inspector
General
United States Postal Service
1735 N. Lynn Street
Arlington, VA 22209-2005
☎888-USPS-OIG (888-877-7644)

Acronyms and Abbreviations Glossary

Acronym/Abbreviation	Definition
Academy	Inspector General Criminal Investigator Academy
AID	Agency for International Development
ARC	Appalachian Regional Commission
APHIS	Animal and Plant Health Inspection Service
CDL	Commercial Drivers License
CFTC	Commodity Futures Trading Commission
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CNCS	Corporation for National and Community Service
CPSC	Consumer Product Safety Commission
CPB	Corporation for Public Broadcasting
Customs	U.S. Customs Service
DCIS	Defense Criminal Investigative Service
DDS	Disability Determination Service
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
E-Government	Electronic Government
EPA	Environmental Protection Agency
ERMS	Earnings Record Maintenance System
FAA	Federal Aviation Administration
FAM	Financial Audit Manual
FBI	Federal Bureau of Investigation
FCA	Farm Credit Administration
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FEC	Federal Election Commission
FEMA	Federal Emergency Management Agency

Acronym/Abbreviation	Definition
FFIS	Foundation Financial Information System
FHA	Federal Housing Authority
FHFB	Federal Housing Finance Board
FLRA	Federal Labor Relations Authority
FMC	Federal Maritime Commission
FRB	Federal Reserve Board
FSIS	Food Safety and Inspection Service
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GPEA	Government Paperwork Elimination Act
GPO	Government Printing Office
GPRA	Government Performance and Results Act
GSA	General Services Administration
HHS	Department of Health and Human Services
HMNLC	Hermanidad Mexicana Nacional Legal Center
HRDN	Human Resources Data Network
HUD	Department of Housing and Urban Development
I&E	Inspections and Evaluations
IG	Inspector General
IGATI	Inspectors General Auditor Training Institute
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
IT	Information Technology
ITC	International Trade Commission
JTTF	Joint Terrorism Task Force
LSC	Legal Services Corporation
NARA	National Archives and Records Administration
NASA	National Aeronautics and Space Administration
NCUA	National Credit Union Administration
NEA	National Endowment for the Arts
NEH	National Endowment for the Humanities
NLRB	National Labor Relations Board
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation
OCSE	Office of Child Support Enforcement
OGE	Office of Government Ethics
OIG	Office of Inspector General

Acronym/Abbreviation	Definition
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSC	Office of Special Counsel
PBGC	Pension Benefit Guaranty Corporation
PC	Peace Corps
PCBs	Polychlorinated Biphenyls
PCIE	President's Council on Integrity and Efficiency
PDD	Presidential Decision Directive
RRB	Railroad Retirement Board
RSM	Retirement Systems Modernization
SBA	Small Business Administration
SBU	Sensitive But Unclassified
SEC	Securities and Exchange Commission
SI	Smithsonian Institution
SSA	Social Security Administration
SSN	Social Security number
TIGTA	Treasury Inspector General for Tax Administration
Treasury	Department of the Treasury
TVA	Tennessee Valley Authority
UCMJ	Uniform Code of Military Justice
USDA	Department of Agriculture
USPS	U.S. Postal Service
VA	Department of Veterans Affairs

Vision

The President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) are effective and influential forces in identifying vulnerabilities in government programs and operations and facilitating excellence in government by recommending needed performance and management improvements. The Councils will lead and promote integrity, accountability, and excellence in governance through effective coordination and enhancement of our efforts to prevent and detect fraud, waste and abuse throughout government.



Mission

Our mission is to independently anticipate and communicate the weaknesses and vulnerabilities of the government, facilitate solutions, and identify opportunities for improved performance by coordinating governmentwide and multi-agency activities that promote economy and efficiency in programs and operations.



**A Progress Report to the President
PCIE ECIE 2001**

