

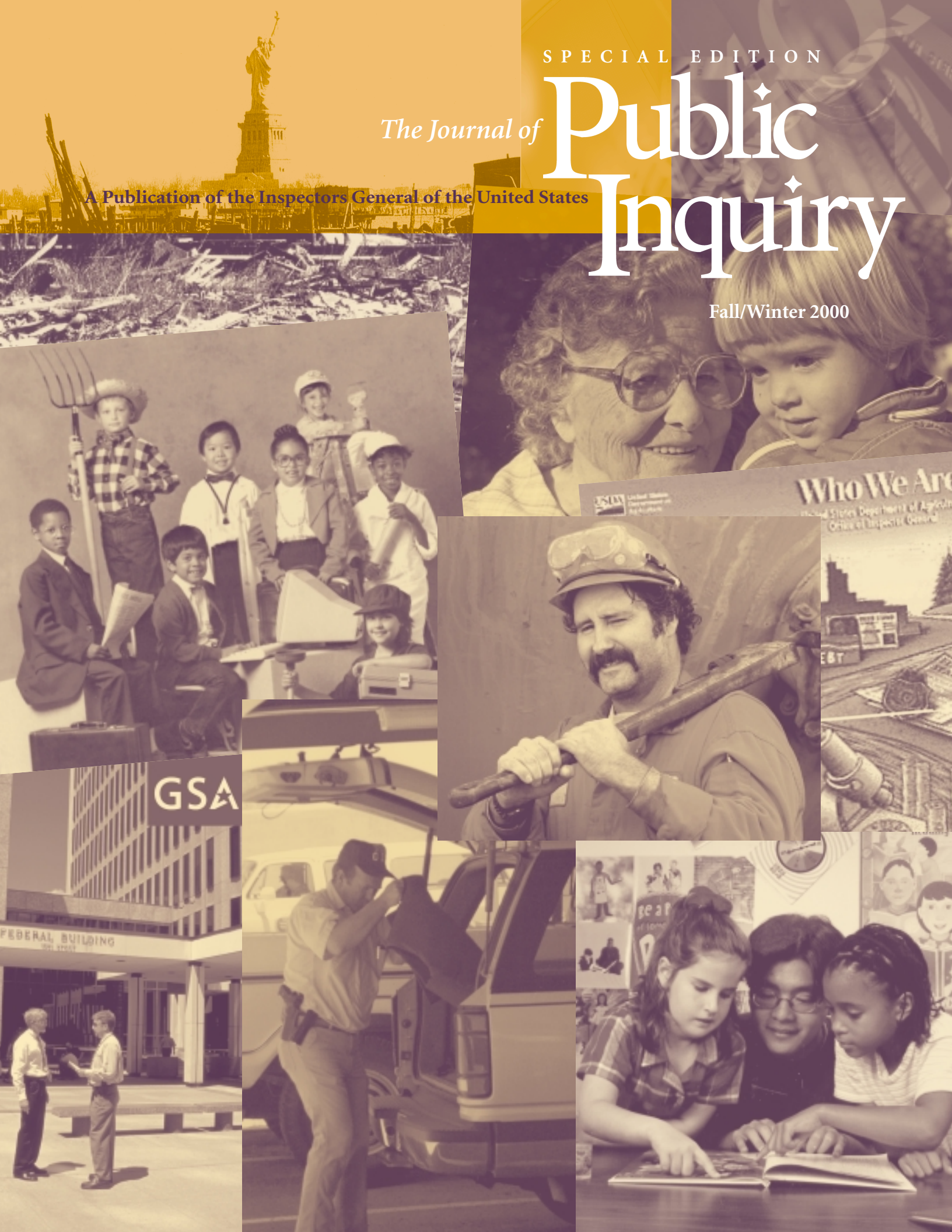
SPECIAL EDITION

The Journal of

Public Inquiry

A Publication of the Inspectors General of the United States

Fall/Winter 2000



EDITORIAL BOARD

Aletha L. Brown, Equal Employment Opportunity Commission, Office of the Inspector General (OIG)

Stuart C. Gilman, Office of Government Ethics

Maryann Grodin, Nuclear Regulatory Commission OIG

Elaine Kaplan, Office of Special Counsel

Joseph R. Willever, Office of Personnel Management, OIG

David C. Williams, Treasury Inspector General for Tax Administration

Karen M. Shaffer, Office of Management and Budget

STAFF

Editor-in-Chief

David C. Williams, Treasury Inspector General for Tax Administration

Editor

Agapi Doulaveris, Treasury Inspector General for Tax Administration

Printing

Department of Defense OIG

Treasury Inspector General for Tax Administration

Design & Layout

Gaston L. Gianni, Jr. & Sharon C. Tushin, Federal Deposit Insurance Corporation OIG

INVITATION TO CONTRIBUTE ARTICLES

The Journal of Public Inquiry is a publication of the Inspectors General of the United States. We are soliciting articles from participating professionals and scholars on topics important to the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. Articles should be approximately 3–5 pages, single-spaced, and should be submitted to Agapi Doulaveris, Treasury Inspector General for Tax Administration, Department of Treasury, IG:MS:PI, 1125 15th Street, N. W., 700A, Washington, DC 20005.

Please note that the journal reserves the right to edit submissions. The journal is a publication of the United States Government. As such, *The Journal of Public Inquiry* is not copyrighted and may be reprinted without permission.

NOTICE

The opinions expressed in *The Journal of Public Inquiry* are the author's alone. They do not represent the opinions or policies of the United States or any Department or Agency of the United States Government.

The Journal of

A Publication of the Inspectors General of the United States

Public Inquiry

Special Edition Fall/Winter 2000

TABLE OF CONTENTS

A Message from the Editor-in Chief 1

An Introduction to The Inspector General Community 3

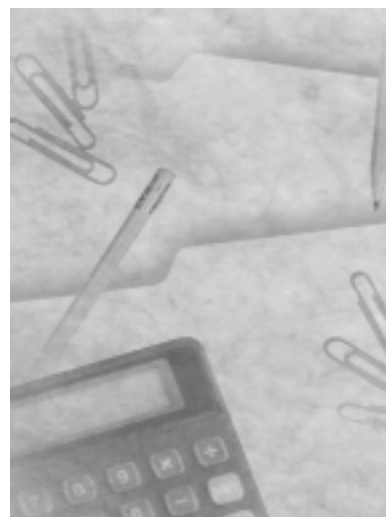
Major Management Concerns



■ Health
Care
9



■ Contracts
and
Acquisitions
15



■ Financial
Audits
12

■ Grants and Loans 18

■ Safety and Environment 21



■ Revenue Protection 24

■ Entitlements 28



■ Integrity of Government Operations 30



■ Information Technology and Security 33

A Message from the Editor-in-Chief

DAVID C. WILLIAMS

We are pleased to present this second special edition of the Journal. This edition focuses on important issues and challenges facing the new administration, as seen from the perspective of the Inspectors General. The issues identified concern the programs that form the backbone of our Federal government, such as defense, health care, and the environment, as well as the ability of our infrastructure to adapt to trends in information technology and financial management.

The success of the Inspectors General (IGs) in every department and agency is dependent, in large part, on developing an effective working relationship with senior management and progressing toward common goals. In the same way, senior managers in these departments often find that their success is dependent on an effective working relationship with the IGs. The job of the new administration coming to Washington is to create and carry out important policy. But together the new administration and the Inspectors General must maintain the confidence of the American people by ensuring that the business of government is conducted in a fair and efficient manner. In government, more than any other sector of our society, the means of developing and implementing policies can be just as important as the policies themselves.

The articles in the first part of this series chronicle the progress made by previous administrations towards reforming Federal programs to ensure their successful administration within the framework of the laws that created them. This Journal chronicles the progress that the Inspectors General, with their unique mission mandated by Congress, hope to make in keeping essential programs efficient, effective, and free of waste and fraud. It should also be a helpful introduction to how working with the IG can help new executives succeed in accomplishing their goals.

Charting the future of these great Federal programs now falls to the officials elected by the people. Those appointed to carry out the work of elected officials must be able to assume stewardship under optimal conditions. In embarking in new directions, there is value in knowing how initiatives have evolved and of past efforts to assure their vitality.

The Inspector General Act that created our offices is a very American law. With this Act, Congress placed an executive within each department and agency to independently assess performance and assure integrity. This does not create a necessarily adversarial relationship between senior management and the IG. Quite to the contrary, many executives have found the independent voice of the Inspector General an asset and assurance of public policy that has been done right and will work. This unique partnership, with two independent entities working toward the same goal, is testimony to the vitality and creativity of American democracy in the 21st century. We wish the new administration well in its efforts to create a body of critical Federal programs—and as Inspectors General we dedicate ourselves to supporting these efforts.

Contributors to the Transition edition of the Journal of Public Inquiry

Bob Ashbaugh, Linda N. Ruder; June Gibbs Brown, Judy Holtz-Rock, Alwyn Cassil; Susan Gaffney; Roberta L. Gross, David M. Cushing, Dana M. Mellerio, Paul J. Shawcross; James G. Huse, Jr., Gerald Hockstein, Shirley Todd, Carolyn Neuwirth, Gale Stone; Donald Mancuso, William P. Goehring; Patrick McFarland, David Cope; Kenneth M. Mead, Jeff Nelligan, Jennifer A. Gavin; Jeffry Rush, Jr., Kathleen Leone, Arthur Henshaw, Dennis Schindel; David C. Williams, Karen Hainer, Margaret Begg, Joseph Ananka, Joanne Wilczynski. 🏠

An Introduction to the Inspector General Community

The civilian Inspectors General (IGs) occupy a unique niche in Federal executive branch agencies. They possess a broad range of independent statutory authorities to examine the efficiency and effectiveness of agency operations as well as to detect fraud, waste and abuse in agency programs. All of the IGs perform two distinct roles: to promote efficient and effective program management and to deter future problems. Their direct customers include agency heads and Congress as well as the program managers and administration officials who act on IG recommendations.

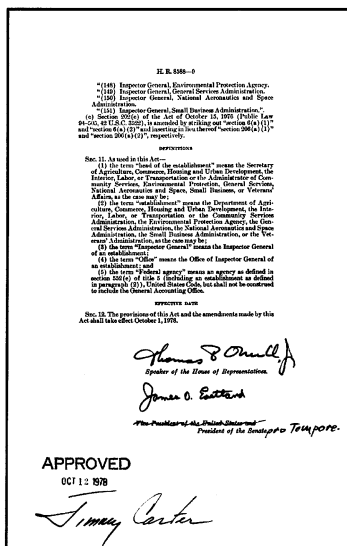
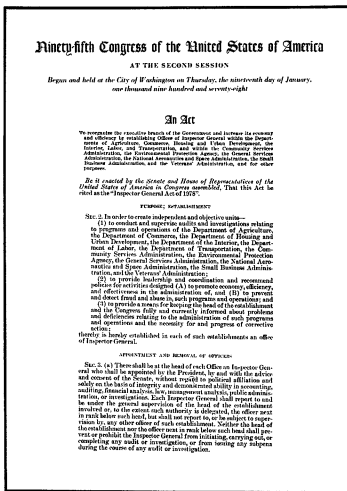
The relationship between an Inspector General and the agency is complex and, because of the IG's statutory authorities, it necessarily differs from the way that the agency interacts with its other components. Properly managed, however, the relationship is almost always mutually productive. The agency receives the benefit of the IG's well-informed and highly objective oversight of its activities, typically generating major management improvements, future operating economies, and significant recoveries of erroneously, improperly, or fraudulently paid funds. In turn, the IG accomplishes its goals of promoting the integrity, economy, and efficiency of Federal government operations much more effectively through a cooperative relationship with the agency. The ultimate beneficiary of a constructive dynamic between the agency and its IG is, of course, the American taxpayer, who receives more effective programs and services from the Federal government at a lower cost.

This article briefly explains the IGs' organization, roles, and accomplishments, and their dealings with their agencies and Congress. The articles that comprise the body of this edition of the *Journal* illustrate the range of the IGs' activities and offer commentary from the IG perspective on the most significant issues likely to face the Federal government during the new administration.

The Inspector General Act

Fraud, waste, and abuse, as well as inefficiency and ineffectiveness, have been historically perceived as significant problems in Federal programs. During the 1960's and 1970's, a series of congressional studies identified a number of systemic shortcomings in the way the executive branch addressed its integrity and efficiency issues, including:

- seriously deficient coordination between agency management and law enforcement officials
- fragmentation and lack of independence of agency audit and oversight components



- inadequate communication among agency auditors, investigators, and program management, even when wrongdoing was discovered
- insufficient public accountability by Federal officials.

These findings became the foundation for the Inspector General Act of 1978, the seminal document of the inspector general community. The Act addressed Congress' concerns by establishing Offices of Inspector General in 12 of the largest Federal agencies. The Act has been amended many times since then, and now provides for IGs in 57 agencies. It remains the cornerstone of every IGs' organizational existence and operations.

Impact of IG Activities

The work of IG offices generates tangible results that benefit Federal programs in many ways. Financially, audits and investigations often provide a basis for recovery of funds that may have been paid erroneously, improperly, or fraudulently. In addition, IG reports identify programmatic improvements that can produce future savings from avoidance of unnecessary costs. The criminal convictions, administrative sanctions, and personnel actions resulting from the IGs' activities represent corrective action directly against persons or entities whose improper conduct has caused loss or harm to Federal programs.

The table below reflects some of the tangible achievements of the 57 IG offices during FY 1991–1999 (the most recent period during which standardized reporting criteria have been used).

Integrity Impact of IG Activities FY 1991–1999

Impact Measure	Total Results
Recommendations in audit reports that costs be disallowed or funds be put to better use	\$106 billion
Financial recoveries resulting from OIG investigative activities	\$13 billion
Successful prosecutions	122,000
Administrative sanctions	47,000
Personnel actions	19,000

Source: PCIE/ECIE Progress Reports to the President, FYs 1991–1999; all numbers cited include results reported by the Office of Inspector General of the U.S. Postal Service, in its oversight role regarding the Postal Inspection Service.

IG Organizational Characteristics and Authorities

While by no means an exhaustive list, IG offices governmentwide reflect the following characteristics and authorities:

Appointment of the Inspectors General: The Act currently provides for IGs in 29 agencies to be appointed by the President, subject to Senate confirmation. These generally (albeit not exclusively) represent the largest agencies. The 1988 amendment to the Act created IG positions to be appointed by the agency head in another 28 agencies. There is no difference in authority or responsibility between the two categories of IGs. Regardless of the appointment authority, Congress must be notified when an IG is removed from office.

Oversight by the agency head only: As a means of assuring that IG activities would receive attention at the highest level of the agency, the Act specified that the IG would be under the general direction of the agency head.

Operating responsibilities and independence: The IGs conduct, coordinate, or oversee all audits and criminal investigations of their agencies' programs. Every IG has full authority

to select, plan, and conduct the work that their offices will undertake. While inclusion of this provision in the Act reflected congressional concerns that the IGs could otherwise be diverted from their statutory role, in practice the IGs always seek agency input regarding the scope and subject matter of their operations. As a further means of protecting the IGs' objectivity, the Act prohibits them from managing any operational program of the agency or supervising the activities of any agency employees outside the Office of the Inspector General.

Access to information: The Act ensures the IGs' access to agency records and personnel to obtain the information needed for audits and investigations. For records located outside the agency, the IGs hold subpoena authority to obtain documentary evidence, which is enforceable in Federal court.

Organization: The presidentially-appointed IGs must designate an Assistant Inspector General for Audits to manage their audit activities and an Assistant Inspector General for Investigations to manage their criminal investigation activities. While not required by statute, almost every presidentially-appointed IG has established a deputy position, filled by a career executive.

IG infrastructure: As a reflection of congressional concerns that the IGs operations could be compromised through administrative action, the Act provided IGs with independent management authority in several areas. For example, the IG has exclusive authority to contract for goods and services, to obtain offices and facilities, and to exercise full personnel management authority for its employees (below the Senior Executive Service level). Funding for the presidentially-appointed IGs is appropriated into a specific account separate from other agency funds. As authorized by the Act, nearly every IG has also established its own office of counsel separate from the agency's general counsel (typically with the agency's full concurrence), to provide legal advice on issues pertaining to audits, investigations, and application of the IG Act.

IG Operations—Audits, Investigations and Related Activities

The Inspector General Act requirement that IGs conduct, control, or review all audit and investigative activities of their agency ensures that efforts to improve integrity and efficiency are appropriately coordinated. Further, as envisioned by the IG Act, the consolidation of employees representing several different professions (auditors, investigators, attorneys, analysts, and other disciplines) in the same organization produces a highly effective, synergistic approach to program integrity issues.

OIG resources are weighted toward the audit function, and are designed to track the agency's activities and focus on performance (i.e., efficiency and effectiveness) and compliance issues. Among the matters that IGs address through their audit programs are:

- determining acceptability of agency financial statements under government auditing standards
- identifying programmatic improvements
- identifying ways that funds could be put to better use
- determining whether contractors or grantees have met their responsibilities to the government
- determining whether agency funds have been paid properly, and
- identifying payments that should be recovered.

With the significant pieces of management reform legislation enacted during the past several years, the IGs also monitor their agency's progress toward improved government performance and greater results for the taxpayer. The IGs' stature within the agency provides for this oversight function and allows the IG to share helpful suggestions and recommendations for overall management improvement as well as legislative compliance.

All IG audit work is designed and conducted so as to comply with the GAO Government Auditing Standards (the “Yellow Book”). The IG community operates the Inspector General Auditor Training Institute, with a curriculum designed to teach both introductory skills and more advanced audit techniques to IG auditors and audit-related staff. The Yellow Book standards serve as a foundation for the training provided by this organization.

The IGs perform criminal and civil investigations of fraud and abuse against their agency’s programs. IGs are required to report suspected violations of Federal criminal law directly to the Attorney General. They work cooperatively, and frequently in task forces or joint projects, with the Department of Justice, the United States Attorneys, and other Federal and state law enforcement agencies on criminal investigations. Virtually all IG criminal investigators exercise law enforcement authority, either through a direct statutory grant to their agency or under deputation by the Department of Justice. Currently, over 2,700 IG criminal investigators hold enforcement powers through these arrangements, including the authority to carry firearms, make arrests, and obtain and execute search warrants.

The IGs’ investigative activities are subject to the government-wide standards and coordination of the Department of Justice. The IG community has also issued quality standards for its investigative activities and operates the Inspector General’s Criminal Investigators Academy, to assure that the quality of IG criminal investigations personnel and practices is equivalent to other law enforcement agencies. A law passed in the 106th Congress provided for establishment of an IG forensics laboratory to assist IG offices in their investigations.

In addition to the audit and investigative activities required by the Act, many IGs have established complementary offices—usually titled as offices of inspection or evaluation—with the capability to provide timely, highly focused analytical studies on particular issues, topics, or programs. The PCIE has also published professional standards for this work, derived from the “Yellow Book” requirements.

Reporting

The principal IG work product is an audit, investigative, or inspection report, normally issued to the official within the agency responsible for the program area addressed by the report. Investigative reports may be sent to a U.S. attorney for prosecutorial consideration or be shared with other Federal law enforcement agencies if they appear relevant to government-wide initiatives. The “Yellow Book” reporting standards may require an audit report to be issued in draft for review and comment before being issued as a final report.

The IG semiannual report is the other cornerstone of IG reporting. It ensures periodic formal reporting to Congress on integrity and efficiency issues by both the IG and the agency. The wide range of mandatory reporting topics reflects Congress’ continuing interest in fostering public accountability on matters related to effective management of Federal programs. The required topics include:

- list of every audit issued during the reporting period
- detailed accounting for several categories of financial impact of audit activities
- narrative summaries of significant audits and investigations
- IG commentary on proposed legislation and regulations which may affect the integrity or efficiency of agency programs
- identification of significant problems, abuses, or deficiencies in the agency
- summary of any instances where the agency declined to provide requested information to the OIG
- identification of matters referred to prosecutorial authorities.

The semiannual report is issued to the agency head, who forwards it to Congress with a separate message, accounting for agency actions in response to IG reports and the

status of unresolved IG recommendations. In addition, the agency may provide its comments on significant efficiency and integrity issues.

Agency Relationships with the IGs

The overall success of the IG concept can be attributed in part to the effective working relationships that have evolved over the years between the IGs and agency heads. These relationships, based on cooperation, mutual respect, and trust, form the foundation for promoting the efficient and effective use of government resources and preventing and detecting fraud, waste, and abuse. While easily said, these relationships are complex and can, at times, be strained by compelling issues that arise. The IGs' ability to maintain an ongoing dialogue and have ready access to the agency head can serve to alleviate some of these inherent conflicts.

In their vision statement, issued nearly a decade ago, the IGs declared themselves to be "agents of positive change," or catalysts, who identify issues and problems that need to be addressed and facilitate positive solutions. IGs are constantly seeking opportunities to have a positive impact on the programs they audit, investigate, or inspect. They strategically plan their work to focus on the greatest risks and top priorities in their particular agency. In this regard, the IG can be a partner in helping the agency head solve the agency's programmatic and operational problems and promoting a more efficient and effective government for the taxpayer.

As with any professional relationship, expectations on both sides must be made clear. Over the years, agency heads have come to rely on the independent review and analyses, based on professional standards, that the IGs bring to bear on difficult and complex issues. However, there are some statutory limitations on the IGs' role, necessary to maintain their objectivity. For example, the IGs, by law, cannot compromise their independence by taking action on their own reports or recommendations, or making or implementing policy decisions about the direction of programs they have reviewed.

Normally, the IG and agency resolve any differences that may arise through ongoing dialogue with each other. However, in the rare instances when it does not appear possible to reach consensus on the resolution of issues identified by audits, investigations, or inspections, the IG may use its ability to report issues directly to Congress as a means of focusing attention on serious problems that it believes require immediate attention.

The overall success of the IG concept can be attributed in part to the effective working relationships that have evolved over the years between the IGs and agency heads.


Government-wide Coordination

The President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE), established by Executive Order, provide coordinating mechanisms for the presidentially-appointed and agency-appointed IGs, respectively. Both groups are chaired by OMB's Deputy Director for Management. They operate in a manner similar to the coordinating bodies for Chief Financial Officers and Chief Information Officers. The PCIE and ECIE address policy issues that cross agency lines, establish professional standards for conduct of IG work, sponsor studies on topics of government-wide concern, and conduct training for IGs, managers, and staff.

As a reflection of the IGs particular concern with accountability and integrity, an Executive Order established a special body, the Integrity Committee, within the PCIE. This entity, chaired by the FBI's Assistant Director for Criminal Investigations, reviews accusations of wrongdoing on the part of IGs and senior executives in IG offices, conducts investigations as warranted, and provides their findings to OMB.

For Further Information

There are a number of excellent sources of additional, detailed information regarding the IG community, its history, and its accomplishments. The following list, while not exhaustive, comprises those that are readily accessible and most frequently consulted within the community itself:

- The semiannual reports produced by each IG
- The PCIE/ECIE Progress Report to the President, compiled on a fiscal year basis, which provide statistical and narrative information regarding the impact of IG activities
- The professional standards applicable to IG work, including the GAO Government Auditing Standards, and the PCIE Quality Standards for Investigations and Quality Standards for Evaluations
- The IGSNet, an extensive website containing much of the information listed above, as well as many other links and references. It can be accessed on the Internet at www.ignet.gov. 

HEALTH CARE

The Government's investment in health care is enormous. One-third of the nation's 1998 trillion dollar health care tab was paid for with Federal dollars. Protecting that investment is a major focus of the Inspectors General at the Departments of Health and Human Services, Veterans Affairs, Defense, and the Office of Personnel Management. From helping to improve quality of care to rooting out fraud, waste and abuse, the Inspectors General play key roles in improving how federally-funded health care is paid for and delivered.

The Offices of Inspector General are statutorily charged with protecting the integrity of their departments' programs, as well as promoting their economy, efficiency and effectiveness. The Inspectors General meet this mandate through comprehensive programs of audits, evaluations and investigations designed to improve the management of their departments. They are charged with ensuring that beneficiaries receive high-quality, necessary services at appropriate payment levels, and preventing waste, fraud, and abuse.

Vulnerability in the Medicare System

Medicare provides health care for the elderly and disabled. With expenditures of \$216.8 billion, it is far and away the largest Federal health care program. Medicaid, a joint Federal and state program for low-income people, is a close second with expenditures of \$170.6 billion in 1998. The Federal portion was about \$100.3 billion, while states contributed about \$70.3 billion. Both Medicare and Medicaid are administered by the Health Care Financing Administration (HCFA), an agency within the Department of Health and Human Services (HHS).

The Medicare program relies on 64 contractors to handle claims processing and administration. The contractors are responsible for paying health care providers for the services provided under Medicare's fee-for-service, providing a full accounting of funds, and conducting activities designed to safeguard the program and its funds. There are two types of contractors: fiscal intermediaries and carriers. Intermediaries process claims filed under Part A of the Medicare program from institutions, such as hospitals and skilled nursing facilities. Carriers process claims under Part B of the program from other health care providers such as physicians and medical equipment suppliers.

Of all the problems observed by the OIG, the most troubling has to do with contractors' integrity—misusing government funds or actively trying to conceal their actions such as altering documents or falsifying statements that specific work was performed. In some cases, contractors have prepared bogus documents to falsely demonstrate superior performance for which Medicare rewarded them with bonuses and additional contracts. In other examples, contractors adjusted their claims processing so that system edits designed to prevent inappropriate payments were invalidated, resulting in misspent Medicare trust fund dollars. The HHS OIG has also encountered problems associated with financial management, accounting procedures and longstanding weaknesses in internal controls including deficiencies related to the receivable amounts reported in HCFA's financial statements and electronic data processing.

There have been numerous allegations that contractors have falsified statements that specific work was performed or altered, removed, concealed, or destroyed documents to improve their ratings on Medicare performance evaluations where wrongdoing has been identified. The OIG has entered into civil settlements with thirteen Medicare contractors since 1993, with total settlements exceeding \$350 million. Additionally, two contractors have entered guilty pleas for obstruction of a Federal audit. With one-third of its contractors under active investigation in fiscal year 2000, oversight of Medicare contractors remains a top priority for the HHS OIG.

There are specific areas of Medicare that are particularly vulnerable to fraud and abuse or quality control problems. This may be due in part to inadequate enrollment procedures for providers, deficient internal controls, excessive payment rates, or especially vulnerable beneficiaries. To illustrate, the OIG continues to be concerned about inappropriate Medicare payments involving mental health services in a variety of settings:

- **Community Mental Health Centers**—In 1998, the OIG completed its five-state study of partial hospitalization services provided in community mental health centers and found that more than 90 percent of the Medicare payments (\$229 million of \$252 million) were for unallowable or highly questionable services.
- **Hospital Outpatient Departments**—The OIG has completed a ten-state review of outpatient psychiatric services at acute care hospitals, estimating that in calendar year 1997 almost 59 percent of the Medicare payments (\$224 million of \$382 million) were for unallowable or unsupported services. OIG is currently completing in-depth reviews of outpatient psychiatric services provided by ten acute care hospitals. This review will indicate whether the Medicare program incurred financial losses because psychiatric hospitals received payments for services and costs that did not meet Medicare eligibility and reimbursement requirements.
- **Mental Health Services in Nursing Homes and Ambulatory Care Settings**—In 1996, the OIG examined the provision of mental health services to nursing facility residents. In 32 percent of the records reviewed, the OIG found that Medicare paid for unnecessary mental health services in nursing homes. The OIG recommended that HCFA take steps to prevent inappropriate payments for mental health services in nursing home settings. In calendar year 2000, the OIG is conducting a follow-up study to determine what steps have been taken as well as conducting a similar study of mental health services in ambulatory care settings.



Health Care Facilities

With expenditures of \$19.4 billion projected for fiscal year 2000, the Department of Veterans Affairs (VA) operates the

nation's largest health system with its 173 medical centers; more than 391 outpatient, community and outreach clinics; 131 nursing home care units and 39 domiciliaries. VA health-care facilities provide a broad spectrum of medical, surgical and rehabilitative care.

With approximately 51,000 medical center beds, VA treats nearly a million patients in its hospitals, 79,000 in nursing homes and 25,000 in domiciliaries. VA's outpatient clinics register approximately 27.5 million visits a year. An estimated 2.5 million individuals receive care annually.

One of the most serious challenges facing the VA is the need to maintain a highly effective health care quality management program that ensures high-quality care and patient safety. This challenge is made even more difficult as the VA shifts care from inpatient hospital settings to ambulatory care and outpatient primary care settings. The more rapid pace of ambulatory care presents increased opportunities for clinicians to make errors in treating patients. The health care industry, including the Veterans Health Administration (VHA), has not yet devised effective ways to quickly and accurately identify and correct such treatment errors. Thus, while patients are less vulnerable to hospital-acquired pathogens, they are increasingly vulnerable to other medical treatment errors and threats to their safety in the ambulatory care setting.

Additionally, the VA has been unable to provide strong and consistent clinical quality management leadership at all levels of the organization. No two VA medical center quality management departments focus on the same issues in the same way. Functional and resource disparities severely impede the agency's ability to identify or measure the extent of widespread unsatisfactory clinical care practices or to devise procedures to correct or eliminate such problems.

Meanwhile, patients continue to be injured in the course of their treatment. In particular, mentally or cognitively impaired patients continue to disappear from VA medical centers—several patients have died before searchers could locate them. The Veterans Health Administration has focused initiatives on this issue but the cause and possible resolution of these patient disappearance problems do not appear to be on the horizon.

The VA OIG continues to follow-up with the VHA on these initiatives and the deployment of resources throughout the VHA. Further, quarterly progress reports to implement OIG recommendations are provided to the House and Senate Committees on Veterans' Affairs. The VA OIG has additional work on patient care quality and safety currently underway or planned.

Oversight of the Military Health System

The Military Health System (MHS) operated by the Department of Defense (DOD) costs nearly \$16 billion annually and serves about eight million people through its health care delivery program, TRICARE. TRICARE provides health care through a combination of direct care at military department hospitals and clinics, and purchased care through managed care support contracts. The MHS has dual missions to support wartime readiness and provide health care during peacetime.

This system faces three major challenges: cost containment, transitioning to managed care, and data integrity. These challenges are complicated by the inadequate information systems available to support the MHS.

Cost containment within the MHS is challenged by the continued lack of good cost information combined with significant levels of health care fraud. Lack of comprehensive patient-level cost data has made decisions regarding whether to purchase health care or to provide the care at military treatment facilities more difficult.

Data integrity in management information systems has been a persistent problem that affects both health care program effectiveness and efficiency. The lack of complete and accurate data has resulted in an inability to clearly identify health care costs, identify unit and individual readiness for deployment, and coordinate direct health care with purchased health care. Department management has put considerable emphasis on improved data quality, and significant progress is being made.

To combat health care fraud, the Defense Criminal Investigative Service has developed an active partnership with TRICARE managers to give high priority to health care fraud cases, which comprise a growing portion of the overall investigative workload. As of September 30, 1999, there were 531 open criminal cases in this area.

Transitioning to managed care is a critical element in peacetime health care delivery. The issue is complicated by a lack of understanding about TRICARE, multiple TRICARE programs offering similar but not identical benefits, and increased focus on providing peacetime health care to the aging retiree population. An audit of the TRICARE marketing program showed that while the level of beneficiary understanding of TRICARE is increasing, DOD has provided Service members with incomplete, incorrect or

inconsistent information. Additionally, with increased base and hospital closures and military downsizing, more and more older beneficiaries (those eligible for Medicare but not DOD-purchased health care) find themselves without access to direct care resources. Attempts to address that problem have led to a proliferation of health care demonstration programs that have further confused the eligible population.


There are two ongoing efforts designed to identify peacetime and wartime staffing requirements to support the MHS. As the MHS transitions to managed care, it must ensure that readiness requirements are not negatively impacted by peacetime health care delivery decisions.

Limited Access to Oversee Health Plans

The Inspector General of the Office of Personnel Management (OPM) has oversight for more than 250 health insurance plans participating in the Federal Employees Health Benefit Program (FEHBP) and is tasked with protecting an \$18 billion trust fund. Based on estimates, as much as \$1.8 billion annually could be consumed by waste, fraud, abuse and mismanagement. The OPM OIG will continue to cope with the many dimensions involved in health care fraud by applying its limited investigative resources and working with other OIGs and the FBI.

The OPM Inspector General's ability to investigate and prosecute health care fraud is adversely affected by the exclusion of the FEHBP from certain civil enforcement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which applies to all other Federal health care programs. This exclusion has made it more difficult for the OIG to participate with prosecutors and other agencies' law enforcement officials in cases involving fraud against multiple health care programs. By excluding the FEHBP from HIPAA, the Inspector General is denied tools that would advance overall efforts in eliminating fraud, waste, and abuse. The OPM OIG continues to pursue a solution to this issue.

Continued Oversight Key to Successful Management

With so much money at stake, health care promises to remain an active area for all Inspectors General whose departments administer health care programs. The very nature of Government health programs—providing care to large numbers of people—makes the programs vulnerable to fraud, waste and mismanagement. Ongoing vigilance will be essential to maintaining and improving the integrity and quality of Federal health care programs. 

FINANCIAL AUDITS

Reliable and timely information is essential to ensure adequate accountability, manage for results, and make well-informed decisions. Without this information, the many efforts across the Government to move to performance-based management will not be achieved. Historically, such information has not been available in the Federal government. The combination of the Chief Financial Officers (CFO) Act, the Government Management Reform Act (GMRA), and the Government Performance and Results Act (GPRA) will generate the necessary cost and performance data necessary to effectively run performance-based agencies.

Efforts to Produce Financial Information

CFO Act and GMRA requirements for audited financial statements have presented a challenge for the Inspector General community, compounded in many cases by the lack of additional resources to meet this new responsibility. They have thrust the IG community into a central role in identifying, reporting, and monitoring critical, longstanding financial management deficiencies in the agencies. Much of the focus on these audits has been about whether an agency received an unqualified or “clean” audit opinion. The broader benefit, however, has been to highlight major financial management system deficiencies and material weaknesses in management controls which must be addressed to enable Federal agencies to produce timely and reliable financial information. The IGs must play a constructive role in advancing recommendations and workable solutions. Working in conjunction with agency chief financial officers the IGs must evaluate progress and make suggestions for correcting weaknesses in financial reporting and internal controls.

For the past three years, the IG community has responded to congressional requests for information on the most serious management issues facing each agency. These responses continue to highlight a major challenge with financial management systems improvements in the Federal government. The extent of this problem is underscored by the fact that only two of the 24 executive agencies, based on fiscal year 1999 audit results, met the requirements of the Federal Financial Management Improvement Act (FFMIA). The FFMIA requires agency financial management systems to comply substantially with Federal accounting standards and financial system requirements. It established new requirements for auditors to report on agency compliance with financial management system requirements, too, and requires that agency management correct deficiencies within three years. The Inspector General for each agency is required to report on agency progress in achieving compliance with FFMIA in the semiannual report to the Congress.

Ten years after the enactment of the CFO Act, more than half of the executive agencies have received clean opinions on their financial statements. By comparison, eleven agencies received unqualified opinions in fiscal year 1997. There were only six agencies with unqualified opinions in fiscal year 1996. In some agencies this achievement required extensive, costly, and time-consuming ad hoc procedures to overcome pervasive internal control and system weaknesses. Several agencies have made good progress toward achieving financial management reform goals. Others have resolved certain previously reported financial statement deficiencies. Notwithstanding the notable accomplishments since inception of the CFO Act, many challenges remain to meet the financial management objectives of the statutes. Some examples of the progress and challenges in dealing with steady improvements in financial accountability that agencies have achieved follow.

Producing Timely and Reliable Financial Information

The Department of Defense (DOD)—with its annual budget exceeding \$250 billion and hundreds of billions of dollars in property, equipment and inventory—represents a large percentage of the Federal government’s assets, liabilities and costs. However, DOD and the military services have not been able to produce auditable financial statements. As a result, billions of dollars in property, equipment, and disbursements have not been properly accounted for and liabilities have not been adequately estimated for environmental cleanup or disposal of weapons systems. DOD management recognizes the seriousness of these problems and has improvement initiatives underway.

Since 1994 the Department of Transportation (DOT) IG has been unable to express an opinion on the financial statements of the Federal Aviation Administration (FAA). In fiscal year 1997, the Inspector General could not validate property, plant, or equipment worth approximately \$12 billion. FAA has taken steps to improve its financial management but more needs to be done to produce auditable information.

Within the Treasury Department, the Internal Revenue Service (IRS), which collects most of the Government's receipts of approximately \$1.7 trillion, received an unqualified audit opinion in fiscal year 1997—a first time achievement. This was the result of significant audit adjustments and correction of serious internal control weaknesses related to tax receipts, taxpayer data, tax refunds and unpaid tax assessments. The IRS has initiated corrective action. However, many initiatives such as the IRS systems modernization efforts are long-term and will take sustained effort to fully implement.

The rest of the IG community is evaluating the progress of correcting weaknesses in financial reporting and internal controls. With concerted effort, all agency material weaknesses have declined from 309 in 1998 to 271 in 1999. Material non-conformances have declined by one-fourth. Working cooperatively with the General Accounting Office, Inspector Generals are recommending to departmental management the actions necessary for achieving legislative reform goals and supporting the effort to produce the first fully audited consolidated financial statement that will encompass the operations of the entire United States government.

Financial Data with Performance Results

Accountability is enhanced when stakeholders can examine the relationship between agency financial information and program results. Without reliable and timely financial information to determine the full costs of programs, however, the Federal government cannot adequately ensure accountability, measure and control costs, manage for results, or

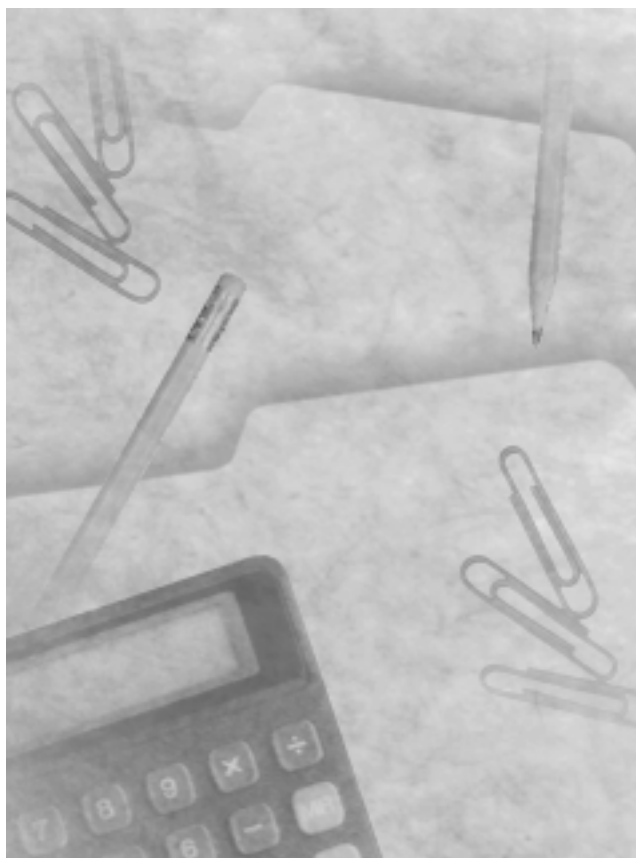
make timely and informed decisions about allocating resources. Under the GPRA requirements for performance measures, program-based cost accounting information will be an invaluable tool for evaluating program efficiency and measuring results.

With the passage of GPRA, Congress has constructed a legislative framework to focus on performance-based management supporting the decision process. New information will be generated to provide a thorough understanding of Federal performance and to help highlight program areas needing attention. The adoption of a results orientation driven by GPRA is key to implementation of

performance-based management. Most agencies are in the early stages of undertaking the changes that performance-based management entails. It is critically important to ensure that the performance and cost information generated be accurate and auditable in order for performance reporting to be credible. There remain many challenges to the Federal government in achieving the full accountability envisioned through GPRA. Following are some examples of GPRA challenges agencies face in achieving full implementation.

The Department of Transportation's first strategic and performance plans were rated by Congress as the best in the Federal government. To build on this success, DOT needs to improve the reliability and timeliness of its performance data. The key GPRA issues

for DOT to focus on are measuring performance and achieving progress that can be documented in the annual performance report and highlighted in DOT's financial statements. The ultimate GPRA test is not collecting data, but actually making progress against performance goals. DOT is challenged by having to accomplish some significant goals through third parties. For instance, the Federal Aviation Administration has a goal for the percentage of runways in good or fair condition. Runway rehabilitation projects are partially funded through FAA grants, but the projects must be initiated by airport operators who pay a portion of the costs, thereby requiring cooperation between FAA and the various airport operators.



The Department of Labor (DOL) currently does not have an integrated strategic management process in which program objectives in strategic plans, the resources appropriated for carrying out the programs, the cost of activities,

Although the Federal government has made major strides over the past ten years, more must be done to ensure that financial management systems and operations are capable of routinely producing accurate, relevant, and timely data to support ongoing program management and accountability decisions.

and the performance results are closely linked. DOL is developing a cost-accounting system. Eventually, cost information will be accumulated for specific activities and performance results. Despite the best efforts, however, it will take years before DOL will be able to achieve linkage. Another challenge is the limited access and control over the quality of program result data needed to determine the attainment of strategic plan goals. This includes difficulties associated with ensuring the quality of data provided by states and other sources below the Federal level.

The Veterans

Administration (VA) has made progress in implementing GPRA but additional improvement is needed to ensure that stakeholders have useful and accurate performance data. Management officials continue to refine performance measures and procedures for compiling data. Yet, the VA

Inspector General continues to find significant problems with data input and weaknesses in information system security—both of which limit management's confidence in the quality of data.

A key challenge for the Treasury Department has been to integrate its GPRA performance planning and reporting activities with its budget formulation and execution activities as well as its annual financial reporting activities as required by the CFO Act and GMRA. Another area of challenge has been for Treasury to develop and implement managerial cost accounting as an integral component of financial and performance reporting. Effective managerial cost accounting is necessary to provide reliable and timely information on the full costs of programs, activities and outputs. This linkage of costs with outputs and outcomes, by responsibility segment and activity, is essential for meaningful reporting as well as cost/benefit analysis under GPRA.

Going Forward

Although the Federal government has made major strides over the past ten years, more must be done to ensure that financial management systems and operations are capable of routinely producing accurate, relevant, and timely data to support ongoing program management and accountability decisions. Until this occurs on a systematic basis, it is imperative that agency heads, chief financial officers, and Inspectors General continue to designate financial management improvements as a top priority. Every effort should be made to ensure management is taking effective and timely actions to correct material weaknesses, particularly to ensure that financial systems comply with FFMIA and continue to improve the credibility of GPRA performance information. 🏠

CONTRACTS AND ACQUISITIONS

Federal agencies rely on private business to provide goods and services that support their programs and activities. Each year, the Government conducts billions of dollars in business with private companies through thousands of contracting actions. To sustain this relationship, it is necessary that business be conducted fairly, that contractors be paid fairly and in a timely manner, and that the Government receive the goods and services for which it contracted.

Acquisition programs and contracting, however, are areas that are vulnerable to fraud, waste and abuse. Offices of Inspector General across the Federal government have identified contracting and acquisition as major management challenges for their agencies. The General Accounting Office (GAO) has also identified the management of large procurement operations as a high-risk area. Specific programs singled out by the GAO as high-risk include:

- Department of Defense Inventory Management
- Department of Defense Weapon Systems Acquisition
- Department of Defense Contract Management
- Department of Energy Contract Management
- Superfund Contract Management
- National Aeronautics and Space Administration Contract Management

It is significant that all but one of these programs has been on the GAO high-risk list since that congressional agency began reporting its high-risk series in 1990 (Department of Defense Contract Management was added in 1992).

The difficulty in effectively managing acquisition programs extends across the Government. The management challenges identified by Offices of Inspector General also confirm that problems in the acquisition process are not isolated to one or two agencies. Management challenges in this area have been identified by large agencies such as the Department of Defense and the Department of Health and Human Services, as well as by smaller agencies such as the Nuclear Regulatory Commission and the Small Business Administration.

Acquisitions is a Major Challenge

The Inspector General at the Department of Defense has identified acquisition as a DOD management challenge. Procurement fraud has been the principal focus of the Defense Criminal Investigative Service, the criminal investigative arm of the OIG, DOD. Major management issues persist concerning the unit cost of weapons systems, contraction of the industrial base, lack of interoperability with allies, material quality and protracted times needed to field new equipment.

Recent reviews by the OIG indicate continuing problems in the department's efforts to comply with acquisition reforms that encourage the use of commercial buying practices. Reliance on market forces to keep prices down works best when competition exists. However, for many DOD procurements competition is limited or nonexistent and audits frequently find the department paying exorbitant prices.

Other recent audits indicate multiple award task order contracts are conferred without regard to price and misused to avoid competition. A particular problem area is in the purchase of services. A recent review of task order contracts found significant errors in all sampled task orders for services. The failure to provide clear guidance and adequate training to contracting officers was identified by the Inspector General as the principle cause for problems in this area. In addition, the DOD acquisition workforce has been cut in half with no proportionate decrease in workload.

Contract Reforms

The Department of Energy (DOE) Inspector General has designated contract management as one of its special emphasis areas. Effective methods for holding DOE contractors accountable are critically important. Of the Department's total budget of about \$17 billion, over \$13 billion is spent by its major operating contractors. The effectiveness of the Department's contract reform efforts of the past several years has been called into question. The DOE Inspector General is particularly concerned with the effort to shift risk, responsibility and accountability to major contractors in exchange for higher fees.

Medicare Oversight

The Department of Health and Human Services (HHS) relies on 64 contractors to handle claims processing and administration for the Medicare program. To promote program integrity, the HHS OIG maintains active oversight of Medicare contractors. OIG investigations of contractors have uncovered misuse of government funds, alteration of documents and falsified statements that specific work was performed.

Medicare contractors are required to have fraud units to detect and deal with problems of fraud and abuse within the health care provider community. OIG review of fraud units found that their effectiveness varies considerably.

The OIG found that some allegations of fraud were masked during the overpayment adjustment process and were not properly developed as potential fraud cases.

Contractor Oversight Blurs Agency Lines

The Department of Housing and Urban Development (HUD) has made significant strides in improving automated systems for accounting and tracking contract status. However, procurement remains one of the top management problems at HUD as identified by the Inspector General. A review by the OIG found that the Contracts Management Review board has not been effectively utilized throughout the procurement process. Additional contracting problems

identified by the OIG included the failure to compare costs and benefits of doing work in-house versus contracting out and awarding "indefinite quantity contracts" using broad statements of work and undefined maximum awards.

Another management challenge for HUD is the Single Family Property Disposition program. The HUD OIG found that the Federal Housing Administration did not have adequate controls in place to oversee its real estate asset management contractors. HUD has since contracted out property disposition activities to management and marketing contractors. The OIG has noted several areas where

these contracts need to be strengthened. Recommendations to HUD include evaluating the performance of contractors in meeting contract objectives, issuing detailed written policies and procedures for approving reimbursement and requiring monetary penalties for recurring contract deficiencies.

The Environmental Protection Agency (EPA) faces management challenges in its oversight of assistance agreements, which are awarded in the form of grants and cooperative agreements to states, local and tribal governments, universities, and nonprofit recipients. EPA regions and headquarters did not know the extent of air pollution problems and could not take appropriate actions to address those problems because significant aspects of work done at the state level was found to be substandard. Second, EPA regions did not clearly com-

municate expectations or monitor state performance. Third, delegated states are not aggressively pursuing formal enforcement action against those facilities in significant non-compliance. Lastly, EPA has had a longstanding practice of awarding grants for which it can only receive incidental benefit, when it should have contracted for work.

NASA, too, faces many procurement and program management challenges. GAO identified NASA contract management as a major management challenge because NASA lacks adequate systems and processes to oversee procurement activities and to produce accurate or reliable management information in a timely manner. A greater reliance on contractors has resulted in problems in areas such as leasing, noncompetitive procurements, subcontract



management, and the use of contractors for on-site support. Additional potential risks exist as the agency moves toward the greater use of electronic commerce, outsourcing, and undertakes other procurement initiatives such as the use of multiple award task order contracts and the Small Business Innovative Research program.

NASA is making the transition to new program management guidelines that were introduced to increase involvement by all parties but place more responsibility with the contractor. The transition period presents risk that noncompliance could occur which will have a material impact on the success of NASA programs. Downsizing the acquisitions workforce and increased reliance on contractor support present further challenges for NASA.

The main challenge of the Nuclear Regulatory Commission (NRC) is to ensure that the civilian use of nuclear materials is conducted in a manner that protects public safety. The NRC has initiated efforts that focus on maintaining public health and safety while reducing unnecessary burden on its licensees. The agency must interface with industry to address concerns regarding new regulatory commitments and performance goals that the industry must satisfy, and must continue to maintain public trust. The NRC is in the process of migrating from traditional procurement methods to electronic commerce to promote an efficient contracting environment.

One of the principal challenges for the Small Business Administration (SBA) is to increase participation in the Section 8(a) program by providing more contracting opportunities to eligible small disadvantaged businesses.

Presently, some companies receive substantial benefits while others receive little or none. This situation exists because the SBA has not determined the level of contract support required to overcome economic disadvantage and because controls are lacking to prevent excessive contract awards.

The SBA also must enforce its rules to limit pass-through procurement activity to non-Section 8(a) participants. Definitive guidance and definitions to evaluate the manufacturing criteria must be established to close existing loop-holes that allow Section 8(a) companies to make minor modifications to a finished product and receive credit with creating a new product. The SBA must ensure that the rules on excessive subcontracting and manufacturing be enforced and develop a formula for calculating labor costs based on a percentage of the total contract value. 🏠

To promote program integrity, the HHS OIG maintains active oversight of Medicare contractors. OIG investigations of contractors have uncovered misuse of government funds, alteration of documents and falsified statements that specific work was performed.

GRANTS AND LOANS

To ensure the efficient use of Government dollars, many Inspectors General have taken a comprehensive approach to keeping the Congress and their agency heads apprised of problems and deficiencies uncovered during their audits and investigations. These IGs have identified areas of high dollar impact or programs in their agencies that, when mismanaged or abused, can most seriously affect those people whom they were intended to serve. The area of grant and loan program administration is one that has been identified by a number of Inspectors General as a priority management issue. Some recent accomplishments, as well as areas needing further attention, are highlighted below.

Improved Debt Management Procedures Could Save Millions

As of September 1999, debt owed to the Department of Veterans Affairs (VA) totaled over \$4.3 billion. This debt resulted from home loan guarantees, direct home loans, life insurance loans, medical care cost fund receivables, compensation and pension overpayments, and educational benefits overpayments.

Over the last four years, the VA OIG has issued 15 audit reports addressing the agency's debt management activities. Recurring themes in these audits attest to the fact that the agency needs to be more aggressive in collecting debts, improving debt avoidance practices, and streamlining and enhancing credit management and debt establishment procedures. These audits (1) identified opportunities to avoid overpayment, establish debt, or improve collection of \$260 million, including \$30.5 million in debts that need to be established; (2) addressed prevention of new debts caused by benefit overpayments of \$81 million annually; and, (3) recommended enhancements to debt collection of nearly \$130 million annually. Through improved collection practices, the VA can increase its receipts from delinquent debt by tens of millions of dollars each year.

Criminal Background Checks on Borrowers

Borrowers who do not disclose past criminal histories have higher rates of default on Small Business Administration (SBA) loans than those that either disclose their records or have no criminal histories. SBA does not have sufficient statutory authority to perform background checks. As a result, losses to the agency are higher than necessary.

Past SBA OIG studies have revealed problems with the accuracy of the criminal history information provided by loan applicants. To determine the extent of the problem, the OIG initiated proactive investigations known as Operation Cleansweep and Cleansweep II. "Operation Cleansweep" showed that almost twelve percent of defaulted loans involved borrowers who failed to disclose their criminal records. After "Operation Cleansweep II", the OIG estimated that based on lending at \$11 billion per year, the potential loss to the Government stemming from these false certifications could exceed \$27 million. Both the Congress and the SBA administrator have expressed support for a more rigorous check of an applicant's criminal history. The Small Business Reauthorization Act of 1997 authorized an expanded check on criminal histories of loan applicants. While useful, the law does not require a background check on every applicant. The OIG believes that verification of criminal history on all loan applicants is the only effective and efficient method available of detecting fraudulent applications early in the loan process, of reducing the Government's losses, and of providing a heightened level of deterrence through increased enforcement actions. The OIG, therefore, recommended legislation requiring that all business loan applicants provide SBA with the information necessary to conduct a criminal background check; and, SBA conduct these background checks on all business loan applicants. Although the SBA supported a change in legislation, the final language passed by the Congress did not confer the necessary authority.

Single Family Loan Fraud Continues to Cost Millions

The Department of Housing and Urban Development (HUD) OIG identified what it found to be the most serious problems facing the agency in a September 1989 report. One of these problems was fraud in the Single Family Mortgage Insurance program. Nearly eleven years later, the OIG again identified risks in the Single Family program as a top

HUD management issue. Recent audit and investigative work, along with housing fraud initiative activities, disclosed that HUD's current procedures for monitoring lenders and oversight of contractors are less than effective.

In one case, 39 individuals involved in a \$110 million fraudulent loan scheme were indicted for their involvement in a "property flipping" scheme, where properties were bought and quickly resold at inflated prices based on fraudulent appraisal values. In this type of scheme, large loans are made based on the inflated appraisals. Sellers and those participating in the scam line their pockets with the extra cash. If the buyer obtains a loan insured by the Federal Housing Administration (FHA) and defaults on the loan, HUD will likely sustain a major loss. In another case, two individuals were charged in a 24-count indictment with obtaining approximately \$30 million in FHA-insured loans through a conspiracy with a mortgage company that involved "strawbuyers" and bogus double escrow accounts.

HUD's mortgage insurance risk depends almost exclusively on the reliability of work performed by its direct endorsement lenders. These lenders underwrite nearly all FHA insurance. HUD mitigates its risk through lender oversight. Three important HUD monitoring tools should be working to prevent the issuance of fraudulent loans: post endorsement technical reviews of loan underwriting documentation, field reviews of appraisals, and, quality assurance reviews of lenders. An OIG audit of HUD's single family loan processes, however, found that HUD monitoring was not focused on lender and appraiser high-risk indicators. The OIG attributes the breakdown in the Single-Family Mortgage Insurance program controls largely to downsizing, inadequate staff expertise resulting from staff reassignments associated with the downsizing, and over-reliance on contractors. There is a clear need for HUD to tighten controls over this multi-billion dollar insurance operation.



Rural Rental Housing Program Susceptible to Abuse

The Rural Rental Housing (RRH) program provides low-cost apartments to people with low incomes in rural areas. Nationwide, there are approximately 447,000 RRH units. Apartment complexes pay an estimated \$161 million in

authorized management fees each year to owners and management agents. In fiscal year 1998, the Government provided over \$1.3 billion in rental assistance and interest credit subsidies for RRH tenants. The Department of Agriculture (USDA) currently has over \$12 billion invested in RRH properties through its outstanding loans.

The Rural Rental Housing Program is vulnerable to program fraud and abuse because of the large cash flows involved. The USDA OIG has worked with the Rural Housing Service to detect fraud and abuse and remove from participation those who abuse the program, and has taken a team approach to identifying and acting on the worst offenders. Additional efforts to improve the RRH Program will result in better program regulations to develop a loan classification system to identify and prioritize "at risk" properties as well as identity-of-interest relationships.

Monitoring of Grant Program Under Review

The Violent Crime Control and Law Enforcement Act of 1994 (Crime Act) authorized the attorney general to implement an \$8.8 billion grant program for state and local law enforcement agencies to hire or deploy 100,000 additional officers to perform community policing. This infusion of funds into the Department of Justice (DOJ) resulted in a management challenge in properly dispensing and monitoring Crime Act funds.

As DOJ becomes more of a grant-making agency, the OIG has directed a significant portion of its resources to auditing grants and grants management by DOJ components. Past OIG audits found that many grantees did not submit required program monitoring and financial reports and that program officials' on-site monitoring reviews did not consistently address all grant conditions. In fiscal year 2000, the OIG is continuing to concentrate audit resources on assessing the effectiveness of DOJ grant monitoring to ensure that individual grantees at the state and local levels are using Crime Act funds to meet the objectives for which they were provided.

Efforts Underway to Ensure Accountability Over Billions in Grant Funds

The Employment and Training Administration (ETA) is the Department of Labor's (DOL) largest grant and contract

awarding agency. ETA awarded \$10.3 billion in grants and contracts in 1998. These funds pay for employment and training programs and services as well as for the administration of unemployment insurance programs run by states.

The DOL OIG has concerns about the ETA's grant process in the areas of cost data and accountability for debt activity. Regarding cost data, the existing ETA system was not year 2000 compliant. However, ETA abandoned the development of a new grants accounting and management system because it would not be completed by the required due date for year 2000 compliance. Procedures were developed to enter all grants activity directly into DOL's general ledger system. But, the OIG financial statement audit for fiscal year 1999 found that significant numbers of cost reports had not been entered into the system. As a result, the year-end grant accrual which is intended to record costs incurred by grantees but not yet reported to DOL, increased from 35 percent of total grant costs to about 65 percent. The OIG's major concerns regarding accountability for debt activity are that the accounting system for ETA debts has not been kept current and that it does not allow for tracing transactions to source documents. These concerns are compounded by the fact that ETA is now responsible for awarding and monitoring millions of additional grant dollars for the Welfare-to-Work program.

The DOL OIG has undertaken a number of efforts to help ensure better accountability over DOL grant funds. These proactive efforts include conducting audits and investigations that identify vulnerabilities and recommending corrective actions before funds are misspent as well as providing technical assistance to grantees.

Millions in Grant Monies Need Improved Monitoring

The Environmental Protection Agency (EPA) accomplishes its mission in large part through assistance agreements awarded in the form of grants and cooperative agreements to states, local and tribal governments, universities, and nonprofit recipients. During fiscal year 1998, EPA awarded more than \$4 billion in assistance agreements—which was more than 50 percent of the agency's budget. Therefore, it is important that the agency and the public receive that for which they have paid.


EPA annually awards more than \$160 million in grants to states to prevent and control air pollution. States use these funds for activities such as inspecting and monitoring facilities, identifying and reporting those facilities not in compliance with the law, and taking appropriate enforcement actions. The EPA OIG found significant aspects of

state work to be substandard, including inspections, reporting, and enforcement programs. Because EPA regions did not clearly communicate expectations or monitor state performance, neither the regions nor headquarters knew the extent of air pollution problems and could not take appropriate actions to address those problems. EPA also awards annual grants to states for the development and implementation of Resource Conservation and Recovery Act (RCRA) hazardous waste programs, including enforcement. The OIG's RCRA enforcement work in 1999 continued to show that delegated states have not consistently ensured that those not in compliance receive timely enforcement actions and return to compliance.

EPA has outlined a number of actions to prevent recurrence of the problems disclosed during OIG audits. Some actions have been completed while others are ongoing. In future audit work, the OIG plans to evaluate the effectiveness of some of these corrective actions. Although the OIG agrees that EPA has addressed certain aspects of these problems, the OIG continues to report this area as a key management challenge because it represents a significant portion of EPA's resources and is critical to the delivery of environmental results.

Grants Management Improved Following OIG Audits

The Federal Emergency Management Administration (FEMA) has made notable strides over the past two years in relation to its grants management. Prior to 1998, FEMA did not have grants management structure that was sufficient to ensure the stewardship of federal funds it awards to states. There were weaknesses in grants awarded for both disaster recovery and emergency preparedness. The FEMA OIG identified deficiencies in FEMA's grant management in a 1995 audit of the Disaster Relief Fund, a 1998 audit of grantee compliance, and three reviews of the cooperative agreement process through which FEMA manages annual grants to states for emergency preparedness. Although improvements are still needed, the OIG is satisfied that FEMA is making a concerted effort to respond to the audit reports and improve its grants management capability.

FEMA's chief financial officer initiated a grants management improvement study in 1997. As a result, the process for managing disaster grants is being reengineered. Training for grant managers is being implemented and the grant closeout process is receiving additional emphasis as well as staffing. Once all the initiatives are in place, the OIG hopes to discontinue identifying grants management as one of FEMA's major management challenges. 

SAFETY AND THE ENVIRONMENT

Ensuring the public safety is among the most basic functions a government performs for its citizens. According to the National Safety Council, more than 92,000 Americans lost their lives in 1998 as a result of unintentional injuries. Further, the total cost of unintentional injuries and deaths that year was \$480.5 billion.

Safety oversight includes the preservation of a clean, livable environment—a task that adds billions per year to taxpayers’ communal bills.

The Offices of Inspector General throughout the Federal government have made public safety and preservation of the environment a key focus of their activities. These goals consistently appear year after year among the top management issues they identify. The OIGs have dedicated substantial time and personnel to addressing issues related to these areas. Several recent actions by Inspectors General are outlined here.

Aviation Safety—Addressing Risk Factors

There were more than 610 million domestic enplanements in 1999. Certainly in the new millennium there will be a continued increase in air traffic. Industry analysts expect that by 2006 there will be more than one billion enplanements. That is why the Federal Aviation Administration (FAA) must aggressively address known risks as well as identify and address the unknown risks that could cause future accidents. New technologies, leading to closer spacing between aircraft due to more precise, satellite-based tracking and navigation capabilities, could prove to be a significant factor in risk reduction. In the past year, the FAA made improvements in several areas.

The FAA implemented “Safer Skies,” a program to reduce commercial and general aviation fatal accident rates. FAA’s new inspection system, Air Transportation Oversight System (ATOS), was initially deployed at eleven air carriers. The agency issued standard operating procedures for reducing the number of runway incursions, defined as near-collisions involving aircraft and other aircraft, objects or people on runways. The Department of Transportation and FAA recognized the need to address safety in the code-share approval process. And the FAA, working with DOT/OIG, continued to pursue the issue of suspected unapproved aircraft parts (SUPs). In fiscal year 1999, FAA initiated 289 SUPs investigations. The Office of the Inspector General obtained 40 indictments related to the sale and use of SUPs. Issues remain, however, for the agency to address:

- FAA needs to follow through and implement procedures to ensure U.S. carriers perform thorough safety assessments of foreign air carriers, now that safety is considered a part of the code-share approval process
- FAA is at risk of not meeting its important safety goal of reducing runway incursions. Additionally, the number of air traffic control operational errors and deviations poses a major threat to aviation safety improvement
- FAA needs to effectively implement its new inspection process, ATOS, for air carriers and improve the accuracy of safety databases
- FAA should move forward to implement the delayed flight- operation quality assurance program in order to advance aviation safety by obtaining better safety data from air carriers
- FAA must issue timely rules that will provide regulatory guidance to the aviation industry. Adoption of new safety practices must be promoted.

Taken as a whole, these recommendations require the prompt and serious attention of the Federal Aviation Administration.

License Transfers and Industry Deregulation

As the Federal government enters the new millennium, agencies are challenged to change with the needs and demands of their stakeholders. Nowhere is that more important than in the area of nuclear license transfers. In December 1998, the Nuclear Regulatory Commission (NRC) issued a final rule amending its regulations to provide uniform procedures and rules of practice for handling requests for hearings associated with license transfer applications. The new procedures are informal and apply to transfers of material and reactor licenses, as well as to licenses issued under regulations governing the independent storage of spent nuclear fuel and high-level radioactive waste. In promulgating this new rule, the NRC noted its expectation that the ongoing restructuring of the electric-power industry will cause a continuing high rate of requests for approval of license transfers. In an increasingly competitive environment, license transfer applications require expeditious decision-making. Moreover, these transfers generally do not involve the kind of technical issues with immediate impact on operating safety that may benefit from review under the complex and often time-consuming formal hearing procedures. The NRC noted its conclusion that the Atomic Energy Act does not require formal, trial-type hearings, but rather gives the agency the flexibility to fashion its procedures to meet the needs of the particular type of decision-making in question. Accordingly, the NRC concluded that for hearings on license transfers uniform informal procedures should be adopted.

Through its regulatory programs, the NRC ensures that civilian use of nuclear materials is conducted in a manner that provides protection of public health and safety. Approximately three million shipments of radioactive waste materials are made each year in the United States. Regulating the safety and security of these shipments, which could be either low or high-level waste materials, is a responsibility shared by a number of different Federal agencies, including the NRC.

To carry out its regulatory responsibilities for high-level spent fuel and non-spent fuel storage and transportation, the NRC certifies transport container package

designs. It licenses and inspects interim storage of spent fuel, both at and away from reactor sites to ensure that licensees transport nuclear materials in packages that will provide a high degree of safety and that licensees provide safe interim storage of spent nuclear fuel. The industry's spent-fuel storage activities, which are expected to increase in significance, require detailed health, safety, and environmental reviews of licensee and vendor procedures and facilities to ensure safe operations.

The reactor license-renewal program evaluates applications to renew current power reactor licenses beyond their expiration dates. It evaluates the effects of aging on materials and safety-related systems, structures, and components. Lastly, it establishes the technical requirements and regulatory framework for renewal of power-plant licenses.

In the new millennium, the transport of these radioactive materials will continue to be a top priority of the NRC.

Safety is the Core Value

Space exploration involves risk, including the risk of failure. Without risk there can be little discovery—and discovery is the National Aeronautic and Space Administration's (NASA) principle mission. To maximize the likelihood of success, NASA must become an informed risk-taker by identifying, understanding, and managing risk as part of

its activities.

The NASA administrator has placed prime emphasis on safety. NASA initiated a program to make the agency the nation's leader in the safety and occupational health of its workforce as well as the safety of the products and service it provides. The agency safety initiative's core process requirements are to promote and ensure safety for the public, astronauts, pilots, employees on the ground, and high-value equipment and property.

Audits and reviews performed by the NASA Office of Inspector General and other organizations support our reporting of Safety and Mission Assurance as a significant area of management concern. A 1999 audit of NASA's safety program management identified issues that could affect the Goddard Space Flight Center's overall safety as well as its preparation for obtaining certification under the Department of Labor's Occupational Safety and Health



Administration Voluntary Protection program. The audit pointed out that the Center's various safety offices are not combined into one organization with a full-time director; haphazard reporting does not ensure that the causes of all accidents are properly addressed or that all accidents are adequately reported, and various contractors' safety records were not evaluated prior to contract award. With respect to combining the Center's various safety offices into one organization, Goddard has consolidated and evaluated leadership of safety through the formation of a high-level safety, health, and environmental council and through complementary management processes. The Center chose this approach rather than an approach that reorganizes safety operations into a single organization. These issues, and particularly contractor safety, will be identified in greater detail during coming audits.

Cleanup of Hazardous-Materials Sites

In the new century the Department of the Interior's (DOI) land-management agencies face a major challenge in cleaning up sites contaminated by hazardous materials, leaking underground storage tanks and pipelines, and illegal dumping. The cleanup costs to DOI have not been determined because of the unknown nature and extent of possible contamination. Furthermore, the DOI's liability for cleanup in relation to other parties has not been established but it is considered potentially significant. The Fish and Wildlife Service, for example, has identified approximately eighteen major sites and ten minor sites on national wildlife refuges and hatcheries, with estimated costs of remediation ranging

from \$103 million to \$120 million. Abandoned mine sites and depleted oil and gas wells cost the Government money, too. Based on an evaluation of its inventory of 3,000 abandoned mines and 727 abandoned oil and gas wells, the Park Service estimates costs of remediation at approximately \$165 million.

The Bureau of Land Management estimates that over 70,000 abandoned mine sites could exist on agency-administered land, for which estimated cleanup liability is not known. The Bureau of Reclamation has identified several potential environmental cleanup responsibilities, including abandoned mines and vehicle-maintenance facilities, and estimates that its potential cleanup liability ranges from \$20 million to \$91 million. Finally, the Bureau of Indian Affairs estimates that its cleanup liability for known sites is \$66 million. It needs approximately \$100 million for studies and evaluations to identify other sites and to determine associated estimates of cleanup costs. DOI has focused its efforts on establishing policies and procedures for waste management, establishing a system to prioritize waste management sites, and is seeking funds to correct identified sites. 🏠

Audits and reviews performed by the NASA Office of Inspector General and other organizations support our reporting of Safety and Mission Assurance as a significant area of management concern.

REVENUE PROTECTION

The Offices of Inspectors General (OIG) have advised Congress that they have identified revenue protection as one of the major challenges facing their departments in fiscal year 2000. The OIGs recommended that revenue could be protected and increased through strengthening both operational and systemic internal controls, as well as the passage of proposed legislation.

Financial Soundness

A major challenge facing the Federal Emergency Management Agency (FEMA) is the financial soundness of the National Flood Insurance Program (NFIP). Since fiscal year 1993, the NFIP has experienced operating losses of approximately \$1.56 billion. This deficit is an indication that the program is not actuarially sound—indeed by design the NFIP does not collect sufficient premium income to build reserves to meet future flood losses. Additionally, the cost to the program of multiple-loss properties is about \$200 million annually. Current FEMA studies and analyses are looking at the impact of eliminating subsidies and reducing the repetitive loss problem.

The second challenge is to improve the coordination and integration of the NFIP with FEMA's new national mitigation strategy. Emphasis needs to be placed on how NFIP and the Hazard Mitigation program can be effectively administered to bring collaboration to these programs. This should include an analysis of how the insurance, mitigation, and compliance components complement each other to achieve both NFIP and mitigation objectives.

Data Matches

An earlier audit report and numerous investigations by the Department of Education OIG provided evidence that underreporting of income by applicants and their parents for student aid is a serious and growing problem. This problem is costing the Federal government hundreds of millions of dollars in awards or excessive awards of Pell Grants to ineligible persons.

The Higher Education Act Amendments of 1998 gave the Education Department the authority to confirm with the Internal Revenue Service (IRS) the adjusted gross income, Federal income taxes paid, filing status and exemptions reported by applicants (including parents) on their Federal income tax returns for the purpose of verifying the information reported by the applicants. The Department of Education is discussing this matter with the IRS.

Agency Solvency

Forecasted demographic changes confronting the nation over the next several decades continue to have a dramatic effect on the future financing of Social Security Administration (SSA) programs. However, the strong performance of the economy and prospects for its future performance has improved the financial status of the combined Social Security trust funds.

Revenues accruing to SSA's two trust funds, the Disability Insurance Trust Fund and the Old Age and Survivors Insurance Trust Fund combined, are now projected to continue to exceed payments for the next 14 years. Beginning in the year 2014, expenditures from the trust funds will exceed tax income and SSA will exhaust the trust funds in the year 2034, a slight improvement from last year's projection. SSA's actuaries estimate that Federal Insurance Contribution Act taxes at that time will support only about 71 percent of the benefits due. To address this issue, the President and the Congress continue to be engaged in a bi-partisan reform effort.

Preventing Medicare Fraud and Abuse

Although payments for medical equipment and supplies represent a small segment of the Medicare program (about \$6 billion), the Health and Human Services (HHS) OIG continues to report on excessive Medicare reimbursement rates and recommended streamlining of fee schedules. The Balanced Budget Act gave the Health Care Financing Administration limited authority to streamline that process which resulted in the Durable Medical Equipment Regional Carriers announcing their plan to reduce fee schedules for several items.

At the present time program changes are needed to correct weaknesses that occur in the way that Medicare assigns and maintains provider numbers. The Balanced Budget Act provided a powerful tool to Medicare by authorizing it to collect social security and tax identification numbers from providers. The Health Insurance Portability and Accountability Act also contained significant provisions related to administrative simplification, which call for a national provider identification system. However, Medicare will not really be secure until these new systems are carefully implemented. The OIG will closely monitor the implementation of the new statutory provisions to ensure that these systems work as intended.

The Medicare payment error rate also is a challenge. In 1998, HHS reported \$176.1 billion in Medicare fee-for-service payments. Previous audits reported that not all claims processed complied with Medicare laws and regulations. These improper payments could range from inadvertent mistakes to outright fraud and abuse. However, internal controls were not effective in detecting the types of processing errors. Continued efforts are needed to reduce the current estimate of over \$9 billion in medically unnecessary and incorrectly coded services.

Federal Crop Insurance Poses Program Challenge

Federal crop insurance has become the U.S. Department of Agriculture's (USDA) farmer "safety net." Between crop

years 1996 and 1999, crop insurance coverage dropped from 205 million acres to 195.6 million, and the Government's total insurance liability increased from \$26.9 billion to \$32.1 billion. This reduction in total acreage coverage coincided with the elimination of required insurance coverage for participation in other USDA programs. For 1999, the Risk Management Agency (RMA) estimated total annual premiums would be about \$2.3 billion. Total 1999 indemnities will probably exceed this estimate due to the disasters and low commodity prices that occurred in the 1999 crop year.

The OIG identified a number of areas where the crop insurance programs need to be strengthened, including oversight and monitoring procedures, verification by loss adjusters, potential conflict-of-interest problems in the multi-peril crop program delivery system, indemnity overpayments resulting from overstated or unreasonable yields, and total liability. Over the past few years, a number of bills have been introduced in Congress directed towards crop insurance reform, but none were enacted.

Financing

The methods of financing the Federal Aviation Administration's (FAA) budget must be changed because of expected increases that are largely due to rising costs in the FAA's operations account. This account represents 60 percent of FAA's fiscal year 2000 budget and is expected to grow to

nearly \$7.6 billion, or about 62 percent of the agency's budget, by fiscal year 2004. The overall FAA budget has increased 73 percent from fiscal year 1998 to fiscal year 2000. FAA estimates that by fiscal year 2004 its budget requirements will be over \$12 billion, or 20 percent greater than fiscal year 2000.

The FAA is subject to the annual appropriations process. Various proposals have recommended alternative approaches for financing FAA, such as user fees, trust fund "firewalls," and guaranteed contributions from the general fund. Regardless of the ultimate financing approach, the FAA must spend and manage its resources more efficiently than in the past. The FAA also must develop the fiscal and



management tools it needs to operate like a business. These include good financial data and reports, a reliable cost accounting system, and a means to control the costs of operations.

Protection of Worker Benefit Funds

The Department of Labor (DOL) administers several programs and statutes designed to provide and protect the benefits of workers. Continual protection of such benefits is critically important because these programs affect the lives of millions of workers and retirees and involve billions of taxpayer dollars. The DOL OIG has identified vulnerabilities within the Department's major worker benefit programs in the areas of unemployment insurance fraud schemes and systemic weaknesses within the programs. The OIG has also proposed legislative action to address the weak-

The Department of Labor (DOL) administers several programs and statutes designed to provide and protect the benefits of workers. Continual protection of such benefits is critically important because these programs affect the lives of millions of workers and retirees and involve billions of taxpayer dollars.

nesses it has identified in the Federal Employees' Compensation Act.

In addition, the OIG is concerned with the escalating indebtedness of the Black Lung Disability Trust Fund. This fund provides disability benefits and medical services to eligible workers in the coal mining industry when a mine operator cannot be determined liable for providing such benefits. The Department's consolidated financial statements for fiscal year 1996 reflected that the trust fund owed \$5.1 billion to the U.S. Treasury. This indebtedness increased to \$5.5 billion in fiscal year 1997, to \$5.9 billion in fiscal

year 1998, and at the close of fiscal year 1999 is approximately \$6.3 billion.

Revenue Collection Can Be Increased

Department of the Interior (DOI) bureaus are involved in numerous activities that generate revenues including mineral lease collections, water use repayments, reclamation fees, resource and material sales, and user fees. Despite collecting over \$8 billion in revenues in 1998, DOI bureaus

can improve the operation of activities that generate revenues and enhance revenue collections. Minerals Management Service can add revenue by prompt confirmation notices and royalty rates and increasing rental revenues by an estimated \$2.4 million to \$26 million for leases. Potential revenues exceeding \$4 million might be obtained from the implementation of recommended concession fee increases and from the assessment of rental fees for concessionaires' use of park housing. Additionally, lost revenues of approximately \$1.3 million result from delays in the re-issuance of expired concession contracts and from the application of lower than recommended franchise fee rates.

The agency reported the failure to effectively inspect fluid minerals and enforce related requirements as a mission-critical material weakness in its 1997 accountability report. The Bureau of Land Management (BLM) reported in its 1998 annual assurance statement, as required by the Federal Managers' Financial Integrity Act, that the material weakness in this activity was corrected. However, the OIG's ongoing audit of the Stripper Oil Well Property Royalty Reduction program disclosed that BLM was not providing sufficient oversight of operators to ensure that information listed on the monthly report of operations was correct regarding the production of oil. As a result, royalties may have been underpaid by as much as \$43 million.

BLM is also responsible for enforcing regulations involving the development, projection, and abandonment of Federal and Indian oil and gas onshore leases. At the end of 1998, there were approximately 20,000 producing onshore oil and gas leases on Federal lands and approximately 3,750 producing leases on Indian lands. Revenues from onshore oil and gas activities were \$873 million for 1998 (latest available). Because of the significance of this activity and the weakness in the inspection of production days reported by operators of stripper wells, further improvements are needed in the inspection and enforcement program.

Strengthening Internal Controls to Increase Revenue Collection

In 1998 the Customs Service collected approximately \$22.1 billion and the Bureau of Alcohol, Tobacco and Firearms (ATF) collected \$12.4 billion in duties, taxes, penalties, interest payments, and fees—the second-largest source of revenue for the Treasury Department. Stronger internal controls and system improvements would increase revenues collected by both bureaus. Customs could significantly reduce lost revenue through its planned large-scale system improvements. This is a major and costly challenge, but would place Customs in a better position to handle electronic commerce and control the hundreds of millions of dollars it collects in user fees and duties. Customs is also faced with an increased workload that is outpacing any

growth in its staffing or funding. Customs continues to rely on its outdated automated commercial system to monitor imported goods and collect billions of dollars in duties and fees. Imports are now valued at nearly \$1.1 trillion per year and are expected to double in five years. Yet Customs, which greatly relies on its computer systems to manage this workload, has serious computer problems that have reduced the bureau's ability to handle its workload.

ATF needs to strengthen its financial management controls in order to ensure that hundreds of millions of dollars in excise taxes do not escape collection. In a recent audit of 17 sampled distilled spirits producers, ATF could potentially have assessed \$66.6 million in additional taxes based on inadequate export data. ATF may not have reviewed other claimed distilled spirits exports, too, with an aggregate tax value of \$560 million for 1996 and 1997. ATF records showed that 73 producers claimed to have exported distilled spirits with a tax value of \$3.25 billion in fiscal year 1998.

Another challenge for Treasury is the estimated hundreds of billions of dollars a year that are laundered globally. The Money Laundering and Financial Crimes Strategy Act of 1998 called for the development of a five-year anti-money laundering strategy. This Act has resulted in increased responsibilities for the Treasury bureaus, especially in Customs and the Financial Crimes Enforcement Network.

Minimizing Tax Filing Fraud

The integrity of Earned Income Tax Credit (EITC) payments has been a concern to the Internal Revenue Service (IRS) as well as to outside stakeholders for many years. Massive EITC scams have been identified in the past and have included conspiracies in which hundreds of taxpayers' social security numbers were used by perpetrators of fraud. An EITC compliance study for tax year 1994 returns found that 25.8 percent of total EITC claimed exceeded the amount to which taxpayers were eligible. More recent research on 1997 tax returns indicates a rise in the EITC overpayment rate. This research is still being validated and will be released late in 2000.

Over the past several years, the IRS has significantly increased its efforts to guard against fraudulent refund claims. For fiscal year 2000, the key to revenue protection efforts has been the preparer outreach campaign that will involve IRS visits to thousands of tax preparers prior to the 2000 filing season to educate them on the requirements when preparing returns claiming the EITC.

Much of the IRS' revenue protection efforts have focused on individual taxpayers reporting wages and withholding rather than business taxpayers. However, there are indications that fraudulent refund claims may be migrating to business returns. 🏠

ENTITLEMENTS

It is easy to understand why improving the management of entitlement payments is one of the most important issues facing Federal agencies and departments charged with administering those payments. Entitlement expenditures are the major component of the entire U.S. budget. The Federal government is expected to spend over \$1.8 trillion in fiscal year 2001. Social Security, Medicare, and other means-tested entitlements will account for an estimated 48 percent of all expected Federal budget outlays.

Every Office of Inspector General (OIG) has as its mission the improvement of its agency's programs by protecting them from fraud, waste, and abuse through independent audits, evaluations and investigations. Each OIG is expected to provide leadership to the agency by making recommendations that promote economy, effectiveness, and efficiency, as well as designing innovative projects that will prevent and detect fraud, waste, and abuse in agency programs. Given this mission and the scope of entitlement outlays, OIGs are devoting significant resources to improving the management of entitlement payments.

Improving the Management of Entitlements

The Social Security Administration (SSA) administers significantly more entitlement outlays than any other Federal agency. In fiscal year 1999, SSA paid approximately \$411 billion in entitlements to about 51 million beneficiaries. SSA's strategic plan includes five goals that affect all programs and their administration. Two of these goals—to deliver customer-responsive service and to make SSA program management the best with zero tolerance for fraud and abuse—often conflict. SSA's policies and procedures requiring evidentiary documentation are a good example of this conflict. If a claims representative takes the time to thoroughly examine the documents presented, this may conflict with the performance indicators tied to prompt delivery of benefits and services. This issue is exacerbated by other factors such as program complexity and growing workloads without commensurate growth in staffing.

Reducing Fraud Vulnerability

To prevent and detect fraud in the disability programs, SSA's OIG designed the "Cooperative Disability Investigation Team" pilot project. This project partners OIG special agents with state Disability Determination Service (DDS) employees and local law enforcement entities. The teams, led by an OIG special agent, typically consist of a SSA claims representative, two state law enforcement officers, and a DDS adjudicator. The success of this project relies on the combined skills and specialized knowledge of these individuals to combat disability fraud in their respective areas. The teams investigate suspicious claims referred by DDS staff. These investigations often result in a denial of initial or continued eligibility for benefit payments. The teams are not only instrumental in weeding out fraudulent claims, they also identify doctors, lawyers, interpreters, and other service providers who facilitate and promote disability fraud. There are currently nine teams operating throughout the nation with two more planned by the end of fiscal year 2000. Since the inception of these teams in 1997, the OIG estimates savings to SSA programs at close to \$40 million.

The General Accounting Office added the Supplemental Security Income (SSI) program to its high-risk list in February 1997. To date it remains on that list. SSA is addressing some factors affecting risk, such as program complexity, and has initiated measures to address its reliance on self-reported data by expanding the range of matches it uses to verify such data. In addition, the OIG has complemented SSA's efforts by establishing SSI fraud initiatives designed to identify ineligible recipients, stop fraudulent payments, recover monies, and pursue administrative and criminal investigations. Investigative projects focus on compliance with residency requirements, payments to deceased beneficiaries, and payments to persons who have not had a recent face-to-face redetermination.

Payment Accuracy

OIG efforts to improve the management of entitlements are not limited to detecting and preventing fraud and abuse. Initiatives that complement agency efforts to improve the accuracy of its benefit payments have been implemented by the OIG. Through a cooperative effort with SSA, the OIG has provided leadership and resources to a SSI payment accuracy task force. This task force reviews the specific causes of payment inaccuracies and recommends changes to the process that will decrease payment errors.

Other Offices of Inspector General have focused on improving the payment accuracy issue as a means to improving management over entitlements.

At the Department of Health and Human Services (HHS), for example, the OIG has conducted reviews in the area of Medicare payments for home health services. There have been dramatic increases in costs for these services. Because of the rapid growth and known vulnerabilities of this program, HHS OIG undertook an extensive body of work, including investigations, audits, and evaluations, and found that inadequate controls resulted in the payment of a high percentage of improper claims. For example, one audit disclosed that 40 percent of the claims in four of the most populated states should not have been reimbursed. OIG findings and recommendations, along with legislative changes and written guidance to home health agencies developed by the OIG, have had a positive impact on reducing error rates.

At the Department of Veterans Affairs (VA), the OIG has conducted several audits reviewing the timeliness and accuracy of benefit payments. A VA OIG audit revealed that agency data on the timeliness of its claims processing was inaccurate, and that actual timeliness data was well below reported. With respect to payment accuracy, the OIG found that the VA needs to develop and implement more effective methods to identify inappropriate benefit payments. Under the Workers Compensation program, for example, payments made to veterans injured as Federal workers are approximately \$140 million annually. The VA OIG audited



this program in 1998 and found that it was not effectively managed. The OIG concluded that by returning current claimants to work who are no longer disabled, the agency could reduce future payments by \$247 million. Additionally, the OIG identified potential fraud cases from a random sample. Based on the results, the OIG found that there were over 500 fraudulent cases being paid about \$9 million annually. Implementation of key actions remain, such as reviewing all open or active cases, and are essential for the agency to strengthen its workers' compensation case management and reduce program costs.

Other OIG reviews of dual compensation cases requiring offsets and payments to incarcerated veterans are examples of reviews that resulted in specific recommendations to address improved management of entitlement benefits.

At the Department of Housing and Urban Development (HUD), OIG reviews have revealed that HUD is not adequately administering the Section 8 Rental Assistance program and continues to experience problems in accounting and budgeting. Recommendations were made to improve tenant income verifications and the accuracy of Section 8 payments, and to analyze the control risks from outsourcing the oversight of the Section 8 portfolio.

Conclusion

Improving the management of entitlements will continue to be a key issue for Federal agencies and departments as well as the Inspector General community. Agencies will continue to place an emphasis on providing beneficiaries with optimum service, such as prompt decisions and timely payments, in a performance-based environment. The Inspector General community needs to ensure that the agency's commitment to provide fast, efficient service is balanced by accuracy and anti-fraud measures. It is critical that OIGs continue to provide strong leadership in fraud prevention, deterrence, and detection through their ability to deliver timely audits, investigations, and inspections that result in real savings to the American public. 🏠

INTEGRITY OF GOVERNMENT OPERATIONS

Underlying all of the management challenges cited by the Offices of Inspector General (OIG) is the understanding that integrity in government operations is essential. Public office carries with it a responsibility to apply public resources economically, efficiently, and effectively. The OIGs' responsibilities include assisting agency management in promoting integrity in program operations. Following are some examples of areas in which OIGs have determined that additional effort will be needed to ensure government integrity.

Maintaining Effective Controls

Management controls are used to provide reasonable assurance that an agency's programs, operations, administrative, accounting, and financial management activities are effectively managed in accordance with applicable laws and that programs achieve intended results. Appropriate internal controls should be applied to all system inputs, processing, and outputs to ensure that resource use is safeguarded against waste, loss, and misuse.

The Social Security Administration (SSA) issued 16 million original and replacement Social Security cards in fiscal year 1999 to U.S. citizens and aliens. Cards are issued based on documents that show evidence of age, identity, and citizenship. Documents that are reviewed include driver's licenses, birth certificates, Immigration and Naturalization Service documents, and current citizenship papers. A SSA OIG audit showed that some applications for a social security number (SSN) have been processed based on false documentation. These occurrences are increasing because the SSN serves as a "breeder document" that is used falsely to obtain other documents such as a driver's license. There is a market for false SSNs that are used by individuals to hide their earnings or to work illegally. Thus, an unscrupulous individual can assume the identity of another person and work using the stolen identity, all the while receiving disability benefits under their own SSN. Individuals also can assume the identity of another person and place their assets under this fraudulent identity in order to qualify for Supplemental Security Income payments under their own SSN.

Passage of the "Identity Theft and Assumption Deterrence Act of 1998" makes document theft a federal crime. This legislation acknowledges that the social security number is a "means of identification" and empowers law enforcement to arrest, prosecute and convict individuals who fraudulently use another person's SSN to create a false identity. The Social Security Administration recognizes the need to enhance its controls over the verification of evidentiary documents submitted with SSN applications. While SSA's initiatives have merit, they tend to concentrate on the detection of fraud rather than its prevention. SSA faces the difficult challenge of balancing anti-fraud measures with its goal of achieving first-class customer service.

Each year, millions of individuals apply for passports and visas at more than 230 U.S. embassies and consulates throughout the world. Attempts to falsify, alter, or counterfeit U.S. visas or passports, or obtain genuine documents by fraudulent means are a constant problem in the United States and overseas. The State Department faces staffing shortages in some high-fraud posts and domestic passport agencies. Further, some staff lack experience and consular line officers are not always properly trained. Problems in the management of anti-fraud programs including a lack of support for overseas post operations, insufficient analysis of data to provide fraud trends and inadequate supervision in anti-fraud units overseas are additional challenges.

The border crossing card, designed to be used in lieu of a passport and visa by Mexican nationals who travel frequently across the border into the United States, has become susceptible to counterfeiting and alterations. Many problems jeopardize the timely implementation of the border crossing card program and compromise its intent to enhance border security. Foremost among them is the Department of State's inability to utilize alternate criminal databases to supplement available databases. Access to a more comprehensive database, such as the one in use by the FBI, is crucial to ensure the validity of laser visa applications and increase U.S. border security. Efforts by the Department of State and INS will be needed to correct these problems.

The Department of Justice's (DOJ) OIG reviewed the Automated Biometric Identification System (IDENT) of the Immigration and Naturalization Service and found that there were serious data management and integrity problems in this enforcement database. These deficiencies could result in the database generating multiple fingerprint identification numbers for the same person. INS has made limited progress in integrating biometrics into its operations. Even in the Border Patrol, where there has been notable progress in using IDENT as a tool for border enforcement, INS needs to integrate IDENT into a comprehensive strategy for battling illegal immigration.

The DOJ OIG has identified numerous mission-critical computer systems that were poorly planned, experienced long delays in implementation, or did not provide timely, useful, or reliable data. The Immigration and Naturalization Service's investment in automation technology and information systems through fiscal year 2001 and beyond is in excess of two billion dollars—an unprecedented expenditure of funds for automation technology that will touch all parts of the agency's operations. In 1998, a DOJ OIG audit found that several major systems were behind schedule and that INS lacked definitive performance measures for tracking critical project milestones. An OIG follow-up audit in 1999 found that INS still could not sufficiently track the status of its projects to determine whether progress is acceptable; INS staff were unable to adequately explain how funds were spent; at least seven automation projects experienced significant unexplained delays; planned project tasks were not adequately monitored to ensure their timely completion; and, progress reports were incomplete, unclear, or untimely.



Security Concerns

Recent reviews by the General Services Administration (GSA) OIG identified deficiencies in security measure implementation in Federal facilities and the reliability of the related management information tracking system. GSA is in the process of implementing recommendations designed to improve this security enhancement effort. Once Federal facilities are brought up to minimum safety standards, GSA's Federal Protective Service (FPS), which is responsi-

ble for developing and coordinating national practices to safeguard life and property in GSA controlled facilities, will need to ensure that adequate personnel are available to carry out its responsibilities. Additionally, GSA must establish an integrated security program that will gather intelligence, maintain technology, and keep a physical presence throughout the Federal and local law enforcement community. Although security enhancements have been made, an OIG follow-up review in 1999 noted that improvements were still necessary concerning the physical installation of security equipment because site inspections identified uninstalled or non-operational countermeasures that had been reported as completed. In addition, management information concerning the security upgrade program was still not completely reliable, despite ongoing corrective measures.

The Department of State recently reported to Congress that its top management concern is ensuring that Department of State personnel and facilities overseas are protected from harm. Improving security overseas will be costly and

require many years of effort. Following the August 1998 bombings of the U.S. Embassies in Nairobi, Kenya, and Dares Salaam, Tanzania, Congress appropriated close to \$1.5 billion in emergency supplemental legislation to cover the costs associated with those bombings and to begin worldwide security enhancements at diplomatic missions overseas. The Department of State OIG is overseeing the agency's use of these funds and providing recommendations to improve security in the immediate and long term. At many of

the facilities, security can be significantly enhanced only through construction of new facilities. The Accountability Review boards estimated that it would cost about \$1.5 billion per year for the next ten years to address known security vulnerabilities. Although sustained capital investment is essential to ensure the future security of the diplomatic infrastructure, it will not immediately alter the circumstances of personnel overseas. Even a major building program will leave the majority of missions vulnerable to some threats for several years.

The U.S. Government controls the export of certain goods and technologies by requiring export licenses for specific dual-use commodities or munitions. Congressional and media attention has focused on the dangers to national security posed by an export licensing process that is alleged

to favor commerce over national security. The defense industry and friendly countries are critical of the current slow and unpredictable license review procedures. The Government needs an export licensing and technology transfer program that protects critical military capabilities through timely and reasonable reviews but also supports Defense cooperation with allies and friends. The Department of Defense (DOD) cannot unilaterally revamp the multi-agency license review process. Attaining interagency consensus in this area is very difficult. Additional challenges facing DOD in this area include determining personnel resource requirements and addressing the marginal adequacy of the Foreign Disclosure and Technical Information System (FORDTIS), the principal automated tool for DOD export control analysts. The audit trail provided by FORDTIS is incomplete, and the review process is insufficiently documented. Additionally, DOD also has no overall

capability to analyze the cumulative effect of exports and other technology acquisitions upon other countries' military capabilities, even though this information is critical to evaluating risks inherent in proposed exports.

In addition to the challenge of preventing unauthorized access by outsiders to information systems, the DOD received new indications during 1999 that its procedures for minimizing security risks from within its own workforce and contractor personnel also needed improvement. The Government Accounting Office (GAO) reported severe problems in both the timeliness and quality of investigations at the Defense Security Service (DSS), which handles DOD personnel security investigations. About 600,000 individuals holding clearances were overdue for reinvestigations in mid-1999. The DOD OIG is following up on the GAO recommendations, which DOD agreed to implement. 🏠

INFORMATION TECHNOLOGY AND SECURITY

The business of government is increasingly dependent on information technology (IT). Along with that dependence comes a vulnerability to disruptions or misuse of IT resources for Federal agencies. Some weaknesses, such as the ability of “hackers” to break into computer systems connected to the Internet, are well publicized. Others, such as the misappropriation of sensitive data from excessed computer equipment or the danger to critical computer systems from natural disasters, have received less attention.

Securing an agency’s IT resources is a growing challenge. While a few Federal agencies have devoted significant resources to IT security, the greater numbers have been slow to recognize the challenge. In this challenging environment, the role of the Office of Inspector General (OIG) is to help the agency through relevant and timely audits, investigations, and inspections, to protect IT resources, and to deter those who would steal information, maliciously shut down systems, or otherwise interfere with the Government’s use of its IT resources. Many of the OIGs have determined that protecting agency IT resources are a priority: 62 percent included IT security and data integrity in their list of top management challenges.

This article reviews some of the key IT security issues encountered by OIGs and discusses the resources their offices need to address IT security.

Compliance with National and Agency IT Rules

Both the President and Congress have created rules concerning IT security. The key national laws and policies are:

- The Clinger-Cohen Act of 1996, which established within Federal agencies the corporate framework for management of information resources, established chief information officers, and called for a comprehensive information technology architecture
- Presidential Decision Directive (PDD) 63, which addresses the protection of critical infrastructures (including physical and computer systems) essential to the minimum operation of the economy and the government
- OMB Circular A-130, which calls for a plan for adequate security of each general Federal automated system and major application as part of the agency’s information resources management planning process.

OIG reviews can determine whether an agency is meeting the requirements of these policies. In addition to examining the agency’s compliance with national policies, an OIG can examine whether the agency is following its own IT security procedures and assess the effectiveness of these procedures.

Protection from Hackers

The vulnerability of Federal agencies to Internet intruders or “hackers” has been well publicized, due to defacements of high profile Federal web sites and malicious widespread virus attacks. Less well known are attempts by hackers to steal passwords, download private files, and disrupt Federal networks. OIGs can make recommendations to their agency’s computer system management and orchestrate the victim agency’s law enforcement response to intrusions. Careful management of computer systems is critical to protecting IT resources from Internet intrusions. OIGs are also well suited to determining whether their agencies are taking the proper steps to protect their computer systems. For example, the National Aeronautics and Space Administration (NASA) OIG conducted several audits of computer systems management at NASA Centers. These audits reviewed whether UNIX-based systems at the Centers met national and NASA guidelines in areas such as protecting and changing passwords, granting system level (root) access, using firewalls, and repairing security holes. The Department of Energy (DOE) OIG conducted

a similar series of reviews at DOE sites. Both OIG reviews recommended changes to improve security.

Another key element in protecting IT resources from intruders is the agency's capability to react to intrusions into its computer systems. The NASA OIG conducted an assessment of the agency's Automated Systems Incident Response Capability (NASIRC) and found that NASA had reduced NASIRC's funding and responsibility, thereby impacting NASIRC's ability to efficiently react to intrusions and to prepare advice and warnings to NASA Centers. Management concurred with the assessment and the eleven OIG recommendations to strengthen NASIRC.

Protection from Viruses

This year's "love bug" and "Melissa" computer viruses disrupted the normal operations of several Government agencies. The damage caused by these types of viruses can be mitigated with a combination of preventative actions, rapid response, and user training. This is a clear situation where an "ounce of protection is better than a pound of cure." OIG reviews to determine whether an agency has taken appropriate steps to defend its computer systems from viruses will be worth the time and effort if these viruses can be assaulted before they do damage.

"Sanitizing" Surplus Hardware

Although Internet intrusions receive much more media attention, critical information can be misappropriated when an agency releases its surplus computers for sale or its obsolete ones for reuse. The NASA OIG found that Privacy Act-protected or other sensitive material could be recovered (using inexpensive commercial utility software) from a majority of surplus computers at one NASA installation. Following this finding, the OIG published an instructional brochure on properly clearing data from hard drives and distributed the brochure throughout NASA and the OIG community. The NASA OIG was not alone in finding problems with excessed computers. The DOE OIG recently discovered that surplus computer hard drives destined for delivery to China were not properly sanitized. The DOE OIG reviewed the sale of an excessed supercomputer,

too, that included 130 disks of unclassified material that had not been properly sanitized prior to the computer's sale.

Physical Security of IT Resources

Another vulnerability that receives too little attention is the physical security of IT resources. The NASA OIG conducted several reviews of the physical security of NASA installations and found that on multiple occasions, unbadged individuals were able to reach computer workstations that were logged into NASA internal networks. The Environmental Protection Agency (EPA) OIG also found that weak physical access controls contributed to poor security in a review of dial-up access to EPA systems. Laptop computers taken outside the agency provide another security vulnerability. Many agencies have had problems with lost or stolen laptops containing sensitive or classified information. Furthermore, the NASA OIG discovered that laptop computers loaned to employees on travel were not sufficiently cleared of information from previous users. An individual could easily retrieve deleted information from a stolen government laptop computer.

Mother Nature can be a threat to the physical security of IT resources, too. The NASA OIG reviewed the disaster recovery plans of mission-critical computer systems at NASA installations particularly vulnerable to natural disasters. In general, the disaster recovery plans did not meet the requirements of PDD 63.

Mother Nature can be a threat to the physical security of IT resources, too. The NASA OIG reviewed the disaster recovery plans of mission-critical computer systems at NASA installations particularly vulnerable to natural disasters. In general, the disaster recovery plans did not meet the requirements of PDD 63.



Outsourcing of IT Capabilities

As Federal agencies lean toward outsourcing their information technology functions, they need to ensure that the IT security function is not compromised. Outsourcing of the desktop and network environments poses a new paradigm for computer operations. Agency information, once physically located on government-owned equipment, now will reside on equipment owned and operated by IT contractors. OIGs can help in this process by ascertaining whether security in IT outsourcing contracts is appropriate. To accomplish this, the OIGs will need sufficient visibility with

contractor operations, including thorough audits and investigations of third-party entities impacting agency operations and programs.

In the rapidly changing IT environment, where new security threats arise as often as new capabilities appear, a Federal agency must have IT security management personnel and policies that are able to address new challenges. OIGs can review whether their agencies' policies are current, whether sufficient personnel are assigned to IT security duties, and whether the IT security function is adequately represented in agency IT organizations, boards, and task forces.

Prosecution of Cyber-criminals

As Federal agencies conduct business, solicit grants and contracts, and purchase supplies electronically, OIGs are responding through their computer crime units. Federal criminal investigators in these units are no longer able to rely on a paper trail to identify their suspect. They trace network intrusions, properly seize computers and electronic media used in the commission of crimes, and retrieve evidence from electronic media.

How Does an OIG Review IT Security?

It is clear that the Inspectors General have a wide range of IT security areas to address. What resources does an OIG need to conduct reviews of its agency's IT security? The answer is complex. Some IT security reviews can be conducted with traditional audit staff. Others require trained IT professionals. Often, an OIG may find that teams with a mix of skills are the most effective in conducting IT security reviews. The NASA OIG, for example, established IT security audit, inspections, and investigation capabilities using agency staff personnel and hiring to fill vacancies created in other program areas:

- The IT audit unit trained in-house auditors and recruited auditors and evaluators familiar with IT. The auditors as a group are now performing ever more complex IT security audits

- NASA's Computer Crimes Division is small but leverages technology to accomplish its work. The OIG recruited skilled staff at high grade-levels in an attempt to remain competitive with the commercial sector. In addition, the OIG trained in-house criminal investigators to supplement the new staff
- The inspections unit began building an IT security review capability by hiring a communications security expert. In-house inspections staff were trained and given field experience to enable them to address complex IT security issues. The inspections unit also receives assistance from the Computer Crimes Division on some complex issues.

Cooperation on IT security between agencies and OIGs can be a powerful approach to protecting Federal assets and resources.

Personnel are not the only requirements for an IT security capability. Although IT security audits rarely require special equipment, a computer crimes unit requires specialized hardware and software to help it read electronic media, perform forensic analysis, and other tasks necessary to bring cyber-criminals to justice.

Conclusion

As the Federal government does more of its business electronically and outsources IT services to the private sector, IT security becomes an increasingly serious issue. Inspectors General can aid Federal agencies struggling to protect their IT resources by providing valuable independent advice and guidance on appropriate levels of IT security. Optimally, heads of Federal agencies should contact their OIG to discuss IT security-related problems and develop an action plan to address these problems. Cooperation on IT security between agencies and OIGs can be a powerful approach to protecting Federal assets and resources. 🏠

Emergency Management

Office of Inspector

IRS e-file



RAIL CROSSING



Merit System Principles

- Recruit qualified individuals from all segments of society and select and advance employees on the basis of merit after fair and open competition.
- Treat employees and applicants fairly and equitably, without regard to political affiliation, race, color, religion, national origin, sex, marital status, age, or handicapping condition.
- Provide equal pay for equal work and reward excellent performance.
- Maintain high standards of integrity, conduct, and character for the public interest.
- Manage employees efficiently and effectively.
- Retain or separate employees on the basis of their performance.
- Evaluate and train employees when it will result in better organizational or individual performance.
- Protect employees from improper political influence.
- Protect employees against reprisal for the lawful disclosure of information in "whistleblower" situations, i.e., protect people who report things like illegal or derelict activities.



SPECIAL EDITION

The Journal of

Public Inquiry

A Publication of the Inspectors General of the United States

Fall/Winter 2000

