

IG's
*Semiannual
Report
to Congress*

September 2002

ENT OF COMMERCE



U.S. Department of Commerce
Office of Inspector General



UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

October 31, 2002

The Honorable Donald L. Evans
Secretary of Commerce
Washington, D.C. 20230

Mr. Secretary:

I am pleased to provide you with the Inspector General's *Semiannual Report to Congress* for the second half of fiscal year 2002. Section 5 of the Inspector General Act requires that you transmit this report, with any comments you may wish to add, to the appropriate congressional committees within 30 days of your receiving it.

This semiannual period marks the end of a fiscal year in which America has faced some sobering, new uncertainties in economic and foreign affairs. Many of these matters directly touch the Department of Commerce—particularly its efforts to support economic expansion and advance U.S. national security, foreign policy, and global competitiveness. This *Semiannual Report to Congress* details our reviews of a number of Commerce programs and activities that pertain to these efforts and reveals a Department committed to its mission and to ensuring the integrity of its operations. We have noted improvement in some areas previously found deficient, while identifying new or persistent weaknesses in other areas that must be addressed. We are confident that with your guidance, your senior officials will continue to pursue resolution of these problems.

One measure of the commitment to this goal is the overall success of the Department at meeting the critical management challenges before it, as identified by my office. You will note that we have revised our list of top challenges to reflect a variety of changing circumstances facing the Department: (1) we combined two challenges related to financial management because Commerce's ability to maintain a clean opinion on its consolidated financial statements depends heavily on its ability to strengthen its financial systems and controls; (2) we changed the focus of our USPTO challenge to reflect the bureau's progress toward transitioning to a performance-based organization; and (3) we have added a challenge that speaks directly to the uncertainties we have come to face in this past year—enhancing emergency preparedness, safety, and security of Commerce facilities and personnel.

This past year—as America has strived to prosper and remain secure—Commerce's responsibility for promoting the nation's well-being, as well as ensuring the security of its own facilities, systems, and personnel, has grown heavier. Our work during this reporting period confirms its determination to fulfill this responsibility. My staff and I look forward to supporting your efforts to ensure the sound management of the Department as it endeavors to meet the many critical missions with which it has been charged.

Sincerely,

A handwritten signature in cursive script that reads "Johnnie E. Frazier".

Johnnie E. Frazier

TABLE OF CONTENTS

IG's Message to Congress	vii
Major Challenges for the Department	1
Strengthen Financial Management Controls and Systems	1
Strengthen Department-Wide Information Security	2
Enhance Export Controls for Dual-Use Commodities	3
Effectively Manage Departmental and Bureau Acquisition Processes	5
Enhance Emergency Preparedness, Safety, and Security of Commerce Facilities and Personnel	7
Successfully Operate USPTO as a Performance-Based Organization	7
Increase International Compliance with Trade Agreements and Expand Market Access for American Exporters	9
Increase the Effectiveness of Marine Resource Management	10
Continue to Improve the Department's Strategic Planning and Performance Measurement in Accordance with GPRA	11
Effectively Manage Major Commerce Renovation and Construction Projects	12
Department of Commerce Organization Chart	13
Agency Overviews	
Bureau of Industry and Security	14
Economic Development Administration	16
Economics and Statistics Administration	26
Minority Business Development Agency	28
National Oceanic and Atmospheric Administration	30
National Telecommunications and Information Administration	38
Technology Administration	39
United States Patent and Trademark Office	45
Department-Wide Management	49
OIG Highlights: Special Items of Note	57
Tables and Statistics	61
Statistical Overview	61
Reporting Requirements	62
Tables and Appendixes	64
Acronyms	70
Types of OIG Reviews	73

IG'S MESSAGE TO CONGRESS

Fiscal year 2002 concludes with America confronting some especially trying times, as the nation and each of its citizens grapple with the new realities that define our security on both foreign and domestic soil. Leaders at all levels of government have been vigilant in their efforts to restore corporate accountability, maintain a stable economy, and ensure the protection of Americans everywhere.

The Department of Commerce plays a pivotal role in promoting economic growth and sustainable development, sponsoring technological innovation, and administering the nation's system for control of dual-use goods and technologies. Accordingly, the Office of Inspector General has spent the past 6 months evaluating the Department's efforts in these and other areas that are critical to its sound and competent functioning. We have noted in many of its programs and activities a strong emphasis on individual and management accountability. We have found continuing dedication to improving the security of the Department's critical assets and some noteworthy progress as a result.

Our emphasis on security, effective management, and accountability during this semiannual period also reflects congressional priorities for all federal agencies. At Commerce these priorities have prompted such work as the following:

National/Systems Security. We conducted our annual follow-up review of actions taken by Commerce units—principally the Bureau of Industry and Security (BIS)—to implement recommendations we have made over the past 3 years for improving dual-use export controls, as required by the National Defense Authorization Act (NDAA) for Fiscal Year 2000 (see page 14). Given the nation's heightened concern about homeland security and the acquisition of weapons of mass destruction by rogue governments and terrorist groups, Commerce's role in setting and implementing dual-use export control policy and regulations will likely remain a priority area for congressional scrutiny, as it will for our office.

Equally important to the national interest is the security of the Department's information assets. Hence, we detail the findings of our Commerce-wide evaluation of information security programs, mandated by the Government Information and Security Reform Act, as well as our agency-specific reviews at the U.S. Patent and Trademark Office (USPTO) and the National Institute

of Standards and Technology (NIST) (see pages 53, 45, and 39, respectively). We are pleased to report that the Department and its operating units have made strides toward improving information security, and we urge them to continue to act on recommendations we have made that remain open. We also discuss the outcome of our evaluation of security provisions in departmental contracts for information services and equipment (see page 51)—a review that uncovered some serious weaknesses in contract documents, which the Department is working to address.

Financial/Operational Management. During this reporting period, we concluded an evaluation of the Department's effort to complete its integrated financial management system, and noted needed improvements in planning and management (see page 52). We reviewed bankcard programs, testified before Congress about Commerce's oversight of purchase card use (see page 57), and collaborated with the Department of Education OIG to produce a guide for conducting effective purchase card reviews (see page 58). We examined operations at the Office of Administrative Services and found that, among other things, its management of the employee awards program was seriously deficient. As a result cash awards sometimes greatly exceeded departmental thresholds, and payroll taxes were not routinely withheld from award payments (see page 49).

Other Areas of Focus. We completed reviews of a range of other departmental activities, such as the following acquisition, financial assistance, and research efforts and, as appropriate, made recommendations:

- **Our assessment of NOAA's high-cost acquisition program to upgrade its fleet of research vessels (page 31)** highlighted a series of weak management controls that threaten to delay ship delivery.
- **Reviews of 19 financial assistance awards made by EDA (page 16), MBDA (page 28), NIST (page 41), and NOAA (page 34)** resulted in our questioning \$3.4 million in federal claimed costs and recommending \$11.2 million in funds to be put to better use. We also identified opportunities to improve management and administration of individual financial assistance programs.
- **An examination of the Salmon Research Plan at the Northwest Fisheries Science Center (page 32)** revealed

that this planning document has many strengths. Whether its implementation will actually improve the quality of the center's salmon-related work, however, has not been rigorously evaluated by a documented peer-review process; such a process could better ensure that the plan addresses program concerns in order of importance. In addition to implementing an effective plan, the center needs to establish better processes for managing research projects and priorities.

You will note that with this *Semiannual Report to Congress* we have revised our list of Top 10 Management Challenges facing the Department to reflect either significant progress, a shifting emphasis, or a new area of concern. Much of the work we describe here corresponds to these challenges and thereby provides a look at Commerce's progress toward resolving them. Accordingly, as implementation of the Commerce Administrative Management System (CAMS) nears completion, we turn to mon-

itoring the Department's continuing efforts to strengthen financial management systems and controls. With acquisition reform well under way, we will now watch how well Commerce manages its procurement processes. And with the U.S. Patent and Trademark Office making steady progress toward incorporating performance-based processes, we will evaluate selected aspects of its operations. Completely new is the challenge to improve and develop the procedures and policies necessary to ensure the safety and security of Commerce facilities and personnel, which will allow the Department to assure the American public that in crisis situations, Commerce functions and responsibilities can and will be carried out.

For all of the work contained in this semiannual report, we have routinely delivered our findings and recommendations to the Department, and it has been generally open and responsive to addressing them. We look forward to detailing its progress at resolving these and other issues in semiannual reports to come.

MAJOR CHALLENGES FOR THE DEPARTMENT

This section highlights OIG's Top 10 Management Challenges that faced the Department at the close of this semiannual period. We view these issues as Commerce's top challenges because they meet one or more of the following criteria: they are important to the Department's mission or the nation's well-being; they are complex; they involve sizable expenditures; or they require significant management improvements. Given the diverse nature of Commerce activities, many of these issues cut across bureau and program lines. We believe that by addressing these challenges the Department can enhance program efficiency and effectiveness; eliminate serious operational problems; decrease fraud, waste, and abuse; and achieve substantial savings.

TOP 10 MANAGEMENT CHALLENGES

1. Strengthen financial management controls and systems.
2. Strengthen Department-wide information security.
3. Enhance export controls for dual-use commodities.
4. Effectively manage departmental and bureau acquisition processes.
5. Enhance emergency preparedness, safety, and security of Commerce facilities and personnel.
6. Successfully operate the U.S. Patent and Trademark Office as a performance-based organization.
7. Increase international compliance with trade agreements and expand market access for American exporters.
8. Increase the effectiveness of marine resource management.
9. Continue to improve the Department's strategic planning and performance measurement in accordance with the Government Performance and Results Act.
10. Effectively manage major Commerce renovation and construction projects.

CHALLENGE 1: STRENGTHEN FINANCIAL MANAGEMENT CONTROLS AND SYSTEMS

The Chief Financial Officers Act of 1990, the Government Performance and Results Act of 1993, the Government Management Reform Act of 1994, and the Federal Financial Management Improvement Act of 1996 were designed to improve financial management and accountability in the federal government. These statutes require the preparation of information needed by Congress, agency executives, and the public to assess management's performance and stewardship. Information required includes audit reports of agency financial statements that present an entity's financial position and results of operations. These reports must state whether an agency's financial management systems comply with federal requirements.

The Department received an unqualified (clean) opinion on its FY 2001 consolidated financial statements—the third consecutive year for this accomplishment despite continuing obstacles, including the absence of a single, integrated financial management system. (See March 2002 issue, page 83). The audits of the Department's FY 2001 statements identified two reportable conditions (one of which is considered a material weakness¹) and several instances of noncompliance with laws and regulations, none of which was a new matter. This number of deficiencies is lower than in previous years as a result of the Department's significant progress in recognizing and recording appropriations, along with improvement in its account balance reconciliations.

Notwithstanding substantial improvements in financial management, maintaining a clean audit opinion remains a major challenge, especially under the accelerated financial reporting dates mandated by the Office of Management and Budget (OMB) for FY 2002 and beyond. Further improvements in financial management systems and operations are essential to enable the Department and its entities to correct the material weaknesses and other deficiencies identified in the audits of FY 2001 statements and produce timely, useful financial information. We

¹ Material weaknesses are serious flaws in the design or operation of an internal control component that increase the risk that errors, fraud, or noncompliance in material amounts may occur and not be readily detected.

retained an independent certified public accounting firm to audit the Department's consolidated financial statements for FY 2002 and will present the findings of this audit in our March 2003 *Semiannual Report to Congress*.

The Department recognizes the need for ongoing efforts to create a financial management environment that provides reliable financial and performance information and complies with federal laws and regulations. Such information is vital to sound decision making. Therefore Commerce continues to focus on strengthening financial management systems by implementing the Department-wide Commerce Administrative Management System to comply with federal laws and regulations and provide Commerce with accurate, timely, and reliable financial management and performance information.

The Department expects that by October 2003, Commerce's outdated and fragmented financial systems will have been replaced by CAMS. While most operating units will use CAMS, three units—International Trade Administration (ITA), U.S. Patent and Trademark Office, and National Technical Information Service—will not, but will submit data along with all other units into a Commerce-wide financial database, which will serve as the source for the Department's consolidated financial reports. The Department expects that CAMS, in conjunction with the database, will bring Commerce into compliance with federal financial systems requirements, including that for a single, integrated financial management system.

Since 1995 the Office of Inspector General has conducted reviews of the CAMS program, assessed the operational system in its annual financial statements audits, and monitored program or system progress. In recent semiannual reports we expressed concern about the management of CAMS development and maintenance, as well as the efficiency and economy of CAMS's implementation. In the last semiannual we noted that, as a result of our reviews of CAMS over the past several years, the Department has taken steps to address many of our recommendations. During this reporting period, we completed our review of program management controls at the CAMS Support Center (CSC) (see page 52). We identified a need for the Department and the center to (1) improve plans for major systems activities to support CSC's budget submission and capital asset planning, (2) track the actual cost of major system activities, (3) improve the *CAMS Capital Asset Plan* and *CAMS Quarterly Reports*, and (4) use an automated management system to monitor cost, schedule, and technical performance.

The Department's response indicates it is taking actions consistent with our recommendations: it is working to improve the CAMS budgeting process as the project moves into the operations and maintenance phase, has begun tracking actual costs as of this fiscal year, intends to improve the quarterly reports, and is working toward a performance-based management system. We will continue to monitor development and implementation of the

Department's financial systems, and will keep Congress and other stakeholders informed of our findings.

CHALLENGE 2: STRENGTHEN DEPARTMENT-WIDE INFORMATION SECURITY

Commerce's information technology systems and the data they process and store are among the most critical assets of virtually all the Department's line offices and operating units. For example, NOAA's satellite, radar, and other weather forecasting data and systems protect lives and property; BIS's export license data helps control the release of dual-use commodities to foreign lands; ESA's economic indicators have policy-making and commercial value and can affect the movement of commodity and financial markets; USPTO's patent and trademark information is essential to administering patent and trademark law, promoting industrial and technical progress, and strengthening the national economy.

Keeping IT systems and data secure is of overriding importance to the Department and the entire nation: loss of or serious damage to any one of Commerce's critical systems could have devastating impacts. However, weaknesses in information security continue to exist throughout Commerce. Thus, identifying those weaknesses and recommending solutions remain a top priority for the Office of Inspector General.

During this semiannual period, OIG completed its second year of information security evaluations under the Government Information Security Reform Act (GISRA), which requires each federal agency to review its information security program annually and each OIG to perform an annual independent evaluation of that program. Agency heads must provide both of these assessments to OMB.

Our evaluation this year found that Department-level executive support for information security continues and has prompted senior management officials in the operating units to increase their attention to this area. As a result the Department has made significant progress over the past year in establishing the foundation for an effective information security program, but much remains to be done, given the severity of Commerce's information security weaknesses and the magnitude and complexity of the effort needed to address them.

For example, we found numerous systems operating without required risk assessments or approved security plans. Some that had approved security plans provided no evidence that risk analysis—a prerequisite for the security plan—had been conducted. Most operational systems have not been accredited (that is, they have not received management's formal authorization to

operate, including its explicit acceptance of risk). Those that are accredited frequently lack evidence of the requisite security testing and evaluation, thus diminishing the assurance that accreditation is intended to impart. We believe that in the coming year, the Department should focus on implementing approved security plans of adequate content and quality for all operational systems and putting those systems through rigorous certification and accreditation processes. The Department reported information security as a material weakness in its FY 2001 *Accountability Report*; we believe it should continue to be reported as such until Commerce systems that are part of the nation's critical infrastructure, as well as those that are mission critical, have been accredited (see page 53).

NIST Evaluation

As part of our Department-wide GISRA review, OIG assessed the information security program at NIST and found that the bureau is taking steps to improve its program but has yet to meet many important security requirements. At the time of our evaluation, NIST lacked a comprehensive information security program policy, did not have a documented risk assessment or approved security plan for any of its operational systems, and had accreditations for only two systems. Since the completion of our fieldwork, the director of NIST has taken important steps toward improving information security, including issuing several memorandums acknowledging responsibility for the security of NIST's data and IT systems and directing all members of senior management to give information security high priority. NIST agreed with the findings in our report and has begun to implement our recommendations (see page 39).

Separate GISRA Review for USPTO

In its efforts to position itself as a performance-based organization—given the greater independence and flexibility provided by the American Inventors Protection Act of 1999 (P.L. 106-113)—the United States Patent and Trademark Office conducts its own information security review and submits its GISRA report separately from the Department. OIG must therefore conduct a separate GISRA assessment of USPTO.

Our independent evaluation found that the Under Secretary of Commerce for Intellectual Property and Director of USPTO has made a commitment to protecting the bureau's information assets and is devoting additional attention and resources to their security. But because of inadequate attention to these matters in the past, significant weaknesses exist in USPTO's planning and budgeting for information security and implementation, review, and oversight of security measures. At the time of our evaluation, more than 80 percent of the bureau's operational systems lacked risk assessments, about one-third had outdated security plans,

and none were accredited. As with Commerce as a whole, we believe that information security at USPTO is a material weakness and should be reported as such until all the bureau's mission-critical systems are accredited (see page 45).

As part of our GISRA review, we assessed USPTO's implementation of system-specific security controls, particularly focusing on the Patent Application Capture and Review System (PACR). The bureau relies on PACR to capture, store, maintain, retrieve, and print digital images of U.S. patent applications and has identified it as a highly sensitive system. We concluded that physical security measures in place during our assessment generally provide appropriate protection for PACR equipment. However, we determined that a risk assessment has not been conducted, the security plan is not approved, security controls have not been tested and reviewed, and contingency planning and specialized security training is needed. USPTO agreed with our recommendations and reported on corrective actions under way or planned (see page 46).

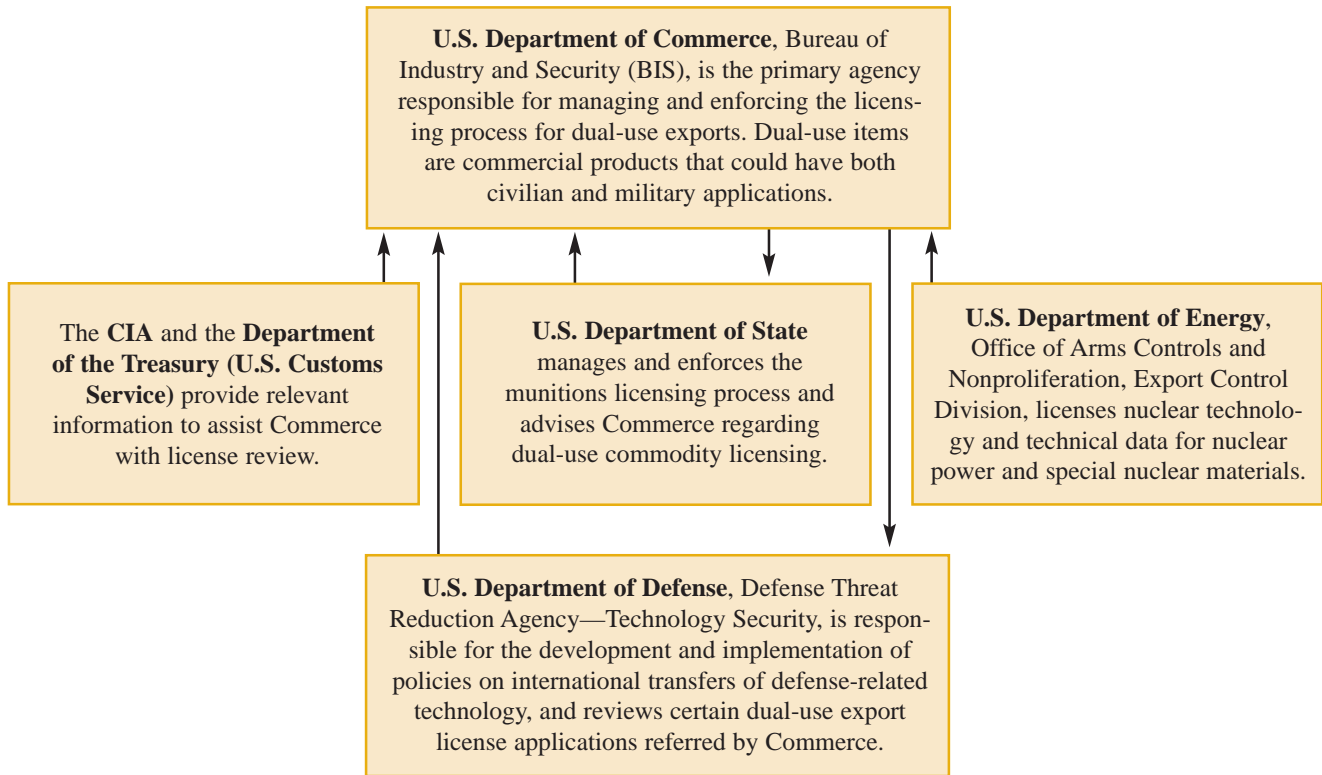
Contract Security Weaknesses

During this semiannual period we also concluded a review of the Department's IT service contracts, finding that security provisions to safeguard sensitive but unclassified systems and information were either insufficient or nonexistent. We recommended that the Department (including USPTO) establish standard contract provisions for safeguarding the security of unclassified systems and disseminate a clear, detailed policy for acquiring these systems and services. We further recommended that the Department determine whether current contracts need to be modified to include information security provisions, recognizing that in some cases contract costs could increase as a result of such changes. The Department agreed with our recommendations and is taking steps to correct the deficiencies (see page 51). We will monitor and report on its progress.

CHALLENGE 3: ENHANCE EXPORT CONTROLS FOR DUAL-USE COMMODITIES

The adequacy of export controls is a continuing concern. Opinions vary on how well the government's export control policies and practices balance the need to protect U.S. national security and foreign policy interests with the desire to promote U.S. trade opportunities and competitiveness. Striking this balance is a significant challenge for the parties involved, particularly for Commerce's Bureau of Industry and Security (BIS), which oversees the federal government's export licensing and enforcement system for dual-use commodities (goods and technologies that have both civilian and military uses).

Federal Agencies Participating in the Dual-Use Licensing Program



Strengthening dual-use export licensing and enforcement requires new, comprehensive legislative authority to replace the expired Export Administration Act of 1979 and appropriately address current export control needs and realities. Passed during the Cold War, the act sought to prevent the export of critical goods and technologies to Communist bloc countries. In today's political climate, rogue countries and terrorist groups seeking weapons of mass destruction and the systems to deliver them pose new threats to U.S. national security and foreign policy goals. Legislation is needed to address these threats, as well as to bolster BIS's regulatory authority, stiffen penalties for violations, and demonstrate America's commitment to maintaining strong export controls while encouraging other countries to do the same.

Given the importance of export controls to national security, we have devoted considerable attention to the challenges facing BIS. Specifically, we responded to a request from the Senate Governmental Affairs Committee to follow up on a 1993 interagency OIG review of the export licensing process. At the conclusion of that follow-up work, we, along with OIGs from the Central Intelligence Agency and the Departments of Defense, Energy, State, and the Treasury, issued a special interagency report in June 1999 on the export licensing processes for dual-use commodities and munitions.

Subsequently, the National Defense Authorization Act for Fiscal Year 2000, as amended, directed the inspectors general of the Departments of Commerce, Defense, Energy, State, and the Treasury, in consultation with the directors of the CIA and FBI, to report to Congress by March 31, 2000, and annually until the year 2007, on the adequacy of export controls and counterintelligence measures to prevent the acquisition of sensitive U.S. technology and technical information by countries and entities of concern. In addition, the NDAA for FY 2001 requires the OIGs to discuss in their annual interagency report the status or disposition of recommendations made in earlier reports submitted in accordance with the act. To date, we have completed three additional reviews of export controls in compliance with the act, as well as three separate follow-up reports.

Although our assessments have identified significant improvements in export controls since 1993, the 1999 report detailed some weaknesses in the licensing process. First, the processes for commodity classification and commodity jurisdiction were not timely and did not clearly specify the role of each agency. Second, the intelligence community did not review all dual-use export license applications or consistently conduct a comprehensive analysis of applications it did review, and license applications were not screened against a key database maintained

by the U.S. Customs Service. Third, there were some recurring problems with BIS's monitoring of licenses that had reporting requirements.

Subsequent OIG reviews have added items to the list of areas that require BIS's attention: the bureau needs to clarify the licensing policy and regulations regarding the release of controlled technology—commonly referred to as “deemed exports”—to foreign nationals. It also needs to conduct more outreach to federal and private research facilities to ensure that they are aware of deemed export regulations and apply for required licenses when appropriate.

The bureau also needs to improve its management of the list of controlled dual-use commodities and technologies, known as the Commerce Control List. We have recommended that BIS make the list more user-friendly, improve the timeliness with which it implements agreed-upon multilateral changes to the list, and address the inappropriate use of national security controls on some items.

Furthermore, we have several concerns about the overall effectiveness of the Committee on Foreign Investment in the United States (CFIUS), specifically CFIUS's lack of mandatory foreign investment reporting, the low number of investigations conducted on company filings, the role of the Treasury in overseeing CFIUS activities, and—within Commerce—the division of responsibilities between BIS and ITA for the CFIUS program.

The interagency OIG review team has agreed to conduct an in-depth examination of the Committee's effectiveness as part of its future work under the National Defense Authorization Act.

Upgrades to Automated Systems

During the last reporting period, we completed a review of BIS's efforts to modernize its automated licensing and enforcement systems. These enhancements are important for the Department because BIS needs a more efficient system for processing export license applications and monitoring/enforcing compliance. Our review found that BIS has made some progress on its systems redesign effort. For example, two components of the system are expected to be implemented in fiscal year 2003. However, our review also determined that BIS needed to (1) better plan to ensure the long-term success of the project and (2) implement established best practices for information technology management.

In addition to our assessment of Commerce's system, the interagency OIG review team looked at the various automated dual-use and munitions export licensing systems—maintained by Commerce, Defense, Energy, and State—to determine whether the systems could better interact and whether system moderniza-

tion initiatives were in accordance with federal policies and regulations. The OIGs found limited effort to coordinate either systems interaction or systems modernization.

In the months since we issued our report on BIS, the bureau has taken action to correct some of the weaknesses we identified. However, OIG recommendations made to the relevant agency heads to help ensure better integration of the licensing systems and avoid duplication may require action by Congress or OMB.

Focused Priorities

The challenges for BIS, as well as for the administration and Congress, remain (1) passing a new Export Administration Act, (2) targeting federal licensing and enforcement efforts on those exports that present the greatest proliferation and national security risks, and (3) streamlining or eliminating controls that unnecessarily hamper trade. We will continue to monitor BIS efforts to improve dual-use export controls through the annual reviews required by the National Defense Authorization Act.

CHALLENGE 4: EFFECTIVELY MANAGE DEPARTMENTAL AND BUREAU ACQUISITION PROCESSES

Federal acquisition legislation in the 1990s mandated sweeping changes to the way federal agencies buy goods and services. Today acquisition reform initiatives are well under way, and the task before Commerce has shifted from successfully implementing reform initiatives to effectively managing the processes those initiatives have fostered. Accordingly, we have revised this top 10 challenge to reflect this new focus.

Effective acquisition processes are critical to the Department: Commerce annually spends more than \$1 billion through contracts and other procurement vehicles. The Department must balance the desire to streamline the acquisition process with the need to ensure that taxpayer dollars are wisely spent and laws and regulations followed.

Acquisition reform was intended to reduce the time and money spent purchasing needed goods and services and improve the efficiency of the process. To accomplish these goals, reform initiatives encouraged contracting officers to (1) rely on performance-based service contracting and use performance-based measurement tools such as earned value and risk management, (2) consider past performance as a criterion for selecting contractors, and (3) make increased use of commercially available products. The initiatives emphasized results-based acquisition

and promoted life-cycle management of information technology as a capital investment. For high-volume, low-dollar purchases, they called for using the government purchase card whenever possible to eliminate lengthy procurement lead times.

The resulting streamlined processes, however, must not neglect basic acquisition principles: careful acquisition planning, prudent review of competitive bids, adept contract negotiations, well-structured contracts, and effective contract management. These are the principles we focus on in evaluating the Department's performance in meeting this top 10 challenge.

Government-wide, the new acquisition methods have brought new concerns. Oversight organizations such as the General Accounting Office (GAO) and OMB's Office of Federal Procurement Policy (OFPP), along with the IG community, report a variety of problems with agencies' implementation of some procurement practices.

- GAO and OIGs have identified problems with some agencies' use of purchase cards, primarily due to weak internal and administrative controls, improper purchases, lack of proper accountability, and inadequate training for cardholders.
- GAO and OFPP have found deficiencies—such as failure to obtain competitive quotes—in the use of government-wide agency contracts (GWACs) and other multiple award instruments.
- With the government's increased emphasis on competitive sourcing, GAO and OFPP remain concerned about the procurement practices of many agencies, criticizing in particular their lack of focus on results.

We also have concerns about service contracting within the Department. In past reports we have identified problems with the use of performance-based service contracting: specifically, failure to use performance-based task orders where they would be beneficial; insufficient planning for contract administration and monitoring; and the need for increased training of contracting officer's technical representatives (COTRs). In this semiannual period, we completed a review of IT service contracts throughout the Department to determine whether they contain information security provisions that adequately safeguard sensitive but unclassified systems and information. (See page 51.) We found that such provisions were either missing or inadequate and recommended that the Department develop policy, incorporate appropriate contract provisions, and require training to help ensure that contracts provide for adequate information security and that acquisition, program, and technical personnel know how to plan, implement, and manage such contracts. The Department

concurred with our recommendations and is taking actions to address them.

The complex nature of certain acquisitions, such as those for performance-based IT services, increases the importance of including the whole acquisition team in the entire contracting cycle—from planning to closeout. Teams should include not only experienced contracting and procurement staff, but also program, technical, security, budget, financial, logistics, and legal personnel. We believe that the inadequacy of security provisions in IT service contracts is attributable, in part, to the lack of sufficient involvement of program managers and IT personnel during acquisition planning, requirements definition, and contract award.

Commerce has continued to implement various reform initiatives and has taken steps to improve acquisition management. Automation of the procurement process has been a primary focus, as has been the qualifications and training of the acquisition workforce. The Department's Office of Acquisition Management (OAM) has focused its attention on strengthening overall management of the procurement function within the Department and the need for additional tools and training for procurement staff. According to the Department, efforts OAM is making to improve management include evaluating Commerce's delegation and warrant program with the goal of realigning contracting authorities to increase overall effectiveness and accountability throughout the Department's procurement community. OAM has reportedly also launched an initiative to restructure the Department-wide certification program for COTRs. This initiative includes a new training plan to enhance COTR performance and the addition of a performance plan element to improve their accountability.

OAM has taken steps to provide oversight and performance measurement of acquisition activities, using a risk management program to monitor the effectiveness of reform initiatives Department-wide. Furthermore OAM completed a review of procedures used by operating units to issue task and delivery orders under General Services Administration (GSA) Federal Supply Schedules and other multiple award contracts and is working on reviews of interagency agreements, memorandums of understanding, and purchase card policy. Finally, OAM is collaborating with the Office of the Chief Information Officer and the Commerce budget office to integrate budget and planning for IT acquisitions. We are currently reviewing purchase card activities. We will discuss our results in the next semiannual report. We will also continue to assess the status of the Department's other acquisition efforts to ensure they meet the goals of acquisition reform. Where necessary we will make recommendations for improvement.

CHALLENGE 5: ENHANCE EMERGENCY PREPAREDNESS, SAFETY, AND SECURITY OF COMMERCE FACILITIES AND PERSONNEL

As the threat of terrorism against U.S. interests has escalated at home and abroad, the need to strengthen security and emergency preparedness in both the public and private sectors has taken on new urgency. Federal agencies have rededicated themselves to ensuring the integrity of their operations, the protection of their people, their ability to continue essential services and operations during a crisis, and the suitability of risk and sensitivity designations² for personnel in positions of public trust. As part of this national effort, the Department has identified and addressed many of the vulnerabilities in its emergency preparedness plans and procedures and in the physical security of its facilities. It is also working to address identified vulnerabilities in its procedures for designating positions according to risk and sensitivity and for conducting appropriate background investigations of the people hired to fill sensitive and security positions. Strengthening policies and procedures to ensure the thoroughness of personnel background checks is an important step that must be taken as departmental managers strive to improve their response capabilities in emergencies and during security threats.

Homeland Security Presidential Directive-3 (HSPD-3), dated March 12, 2002, established a Homeland Security Advisory System for the nation and requires executive branch agencies to implement protective physical security measures to reduce vulnerability or increase response capability during periods of heightened alert. Subsequently the Department issued a memorandum to all Commerce operating units directing senior officials to survey their current safety status and implement any measures required by the directive that are not already in place, along with supplementary measures that local conditions may require.

In addition, Presidential Decision Directive 67, dated October 1998, directs federal agencies to develop continuity of operations plans (COOPs) to ensure the performance of essential functions during any situation that may disrupt normal operations. The chaos of September 11 highlighted the need for each federal agency to have a COOP in place that details the orderly transition to emergency operations and ensures that essential services and functions continue during a crisis, be it generated by terrorist-related incidents, natural disasters, or other events.

² Risk designations reflect the potential damage an individual in a position of public trust could cause to the efficiency and integrity of government programs and operations. Sensitivity designations reflect the potential adverse impact on national security associated with a position.

Complying with these directives, and related ones, is a complex, resource-intensive undertaking for Commerce, given the size of its workforce, its diverse and important missions, and the geographical spread of its approximately 500 facilities across the 50 states and 160 offices overseas. Heightened security requires a variety of measures: infrastructure risk assessments, emergency backup sites, upgraded physical security, and employee awareness and training, to name a few. The Department's personnel are being asked to safeguard life and property under emergency circumstances and to ensure that essential functions continue during any of a broad spectrum of emergencies. We believe that Commerce is making progress on many of these fronts, but the challenge is massive.

In our March 2002 report on the status of emergency preparedness and security programs at a cross-section of Commerce facilities in the Washington, D.C., area and across the nation, we concluded that significant improvements had been made since September 11 in the Department's readiness to deal with future emergencies. However, we noted that significant vulnerabilities still existed. We also identified some significant safety issues at the Commerce headquarters building in Washington, D.C., and in certain NOAA facilities in Seattle, Washington. (See March 2002 *Semiannual Report to Congress*, pages 77-82.)

Commerce's challenge to strengthen emergency preparedness, security, and safety extends to its overseas operations, especially those not collocated with U.S. embassies and consulates. In these latter situations the Department has primary responsibility for the safety and security of its people and facilities. In recent inspections of overseas posts operated by the U.S. and Foreign Commercial Service (US&FCS), we identified the need for more timely security upgrades, better management of resources, and improved oversight of security operations. (See March 2002 issue, page 40, and September 2000 issue, page 47.)

Given the heightened awareness of our vulnerability to acts of terrorism, the Department will have to regularly revisit its procedures for ensuring the safety and security of its employees and operations, and modify them as needed. We will continue to monitor its efforts in this regard and report our findings accordingly.

CHALLENGE 6: SUCCESSFULLY OPERATE U.S. PATENT AND TRADEMARK OFFICE AS A PERFORMANCE-BASED ORGANIZATION

The American Inventors Protection Act of 1999 established the U.S. Patent and Trademark Office as a performance-based organ-

ization, giving it greater flexibility and independence to operate more like a business. As such, USPTO has not only broader responsibility for managing its operations but also expanded control over its budget allocations and expenditures, personnel decisions and processes, and procurement operations.

Despite the act's potential benefits, USPTO's continuing transformation remains a formidable challenge as the agency strives to keep pace with increasingly complex technology and customer demands for higher quality products and services. In June 2002 the bureau responded to the concerns of its many stakeholders by issuing the *21st Century Strategic Plan*, which it believes will help guide the way to meeting the many challenges that have accompanied its transition to performance-based operations. The bureau must continue to develop the necessary personnel, procurement, and administrative policies, as well as performance-oriented processes and standards for evaluating cost-effectiveness, while meeting its performance goals under the Government Performance and Results Act (GPRA) and the timeliness standards of the American Inventors Protection Act.

The 5-year strategic plan, according to USPTO, is aggressive and far-reaching, and provides a road map for major changes in patent and trademark processes. It is intended to (1) reduce patent pendency from the current 25 months to 18 months by 2008, (2) move to a paperless environment and promote e-government, (3) enhance employee development, (4) explore competitive sourcing, and (5) improve and maintain quality control. USPTO's strategic plan also calls for the agency to work with worldwide intellectual property offices to create a global framework for enforcing intellectual property rights.

Agency management believes that failure to implement the new plan will delay USPTO's full implementation of e-government initiatives and increase pendency rates. It should be noted, however, that several of the initiatives envisioned in the plan—outsourcing preexamination reviews and changing fee structures, for example—require congressional approval.

During the next 2 years, we will review some of the operational changes the plan proposes. We view completion of this transition as critical to USPTO's operating success and its ability to address other challenges we identified in recent years, as described below.

Staffing to Handle Changes in Patent and Trademark Application Activity

The number of patent application filings skyrocketed in recent years. In FY 2001 USPTO received more than 326,081 applications for patents—an 8.9 percent increase over the number received in FY 2000. To address the expanding workload, USPTO hired 789 patent examiners, but lost 700 through attrition during

fiscal years 2000 and 2001, virtually negating its efforts to increase staffing. Trademark filings, on the other hand, peaked in 2000 at 375,000 applications, but declined by 21 percent (to 296,000) in FY 2001. Because this downward trend is expected to continue, the bureau has started to downsize its trademark staff.

Our prior audits of USPTO reported on some of the challenges facing the bureau in recruiting and training examiners and in hiring additional administrative judges to hear appeals. As a performance-based organization, USPTO has greater flexibility to design incentives to attract and retain these highly skilled employees. During the last semiannual period we completed a review of attrition problems in two patent examiner work groups (see March 2002 issue, page 71). We made a number of recommendations for improving the screening and hiring process and thereby ultimately improving retention.

Construction of New Facility

USPTO and GSA are currently undertaking one of the federal government's largest real estate ventures—construction of USPTO's 2.4 million-square-foot office complex in Alexandria, Virginia. When completed in 2005, the 5-building complex will provide space for USPTO employees and operations currently scattered among 18 buildings in nearby Crystal City, Virginia. Now that construction has begun, USPTO must aggressively hold the line on project costs, monitor construction progress, and help ensure the project stays on schedule and within the legislatively mandated cap on the cost of completing the build-out of the facility's shell. We will be monitoring this major challenge and will follow up on issues we identified during the project's planning and design, such as space planning and allocation, relocation strategies, and actual versus target costs and completion schedules.



During construction its working title is "Building E," but USPTO will officially name this structure the Remsen Building. It is scheduled to be completed by the end of 2003.

IT Capabilities

USPTO continues to face significant challenges in delivering essential information technology capabilities. The American Inventors Protection Act of 1999 requires greater operational efficiency from the bureau, further intensifying the demands placed on IT solutions and USPTO's ability to develop new and upgrade existing systems. Our March 2002 evaluation of USPTO's information security program found that in general, the bureau's documented policies and procedures are consistent with accepted security practices, but many important security requirements are not implemented, and fundamental responsibilities are frequently not carried out (see March 2002 issue, page 74). USPTO concurred with our findings and has begun implementing our recommendations. While the results of our evaluation suggest that information security has yet to become an integral part of USPTO's business operations, the bureau's response to our recommendations indicates genuine concern about the security of its IT systems and a commitment to a stronger security program (see page 45).

CHALLENGE 7: INCREASE INTERNATIONAL COMPLIANCE WITH TRADE AGREEMENTS AND EXPAND MARKET ACCESS FOR AMERICAN EXPORTERS

To compete effectively in today's global marketplace, U.S. companies need help addressing unfair trade practices, violations of trade agreements, inadequate intellectual property protection, and other impediments to the import and export of goods and services as well as addressing confrontational situations with foreign firms operating in U.S. markets. Commerce must ensure that its trade compliance and market access efforts adequately serve U.S. companies by helping expand trade, open world markets, and eliminate unfair competition from imports priced at less than fair market value or subsidized by foreign governments.

Commerce, through various offices within the International Trade Administration, works with the Office of the U.S. Trade Representative, the Departments of State and Agriculture, and numerous other federal agencies to monitor and enforce trade agreements. The number and complexity of agreements have increased substantially in recent years.

To help in its compliance efforts, ITA created the Trade Compliance Center in 1996. The center monitors U.S. trade agreements and reviews complaints from a variety of sources. When warranted, it forms a compliance team to bring a case to

satisfactory conclusion. Team members are drawn from center staff and other ITA operating units including Market Access and Compliance, Trade Development, the U.S. and Foreign Commercial Service, and other Commerce agencies, as appropriate. In addition to the activities coordinated by the center, ITA's other operating units perform a substantial amount of market access and trade compliance work. Overall, ITA's approach to trade compliance and market access is to try to solve problems at the lowest level possible—avoiding formal dispute settlement structures such as the World Trade Organization, which can take years to resolve trade disagreements.

On the import side, unfair foreign pricing and government subsidies can disrupt the free flow of goods and adversely affect U.S. companies' global competitiveness. ITA's Import Administration (IA) works with the International Trade Commission to enforce the nation's antidumping and countervailing duty laws. IA investigates complaints from U.S. industries against foreign producers and governments to determine whether dumping or subsidization has occurred and, if so, to what extent. The commission determines whether U.S. industry has suffered material injury as a result of the dumped or subsidized products. If both agencies determine that injury has occurred, IA instructs the U.S. Customs Service to assess duties against imports of those products.

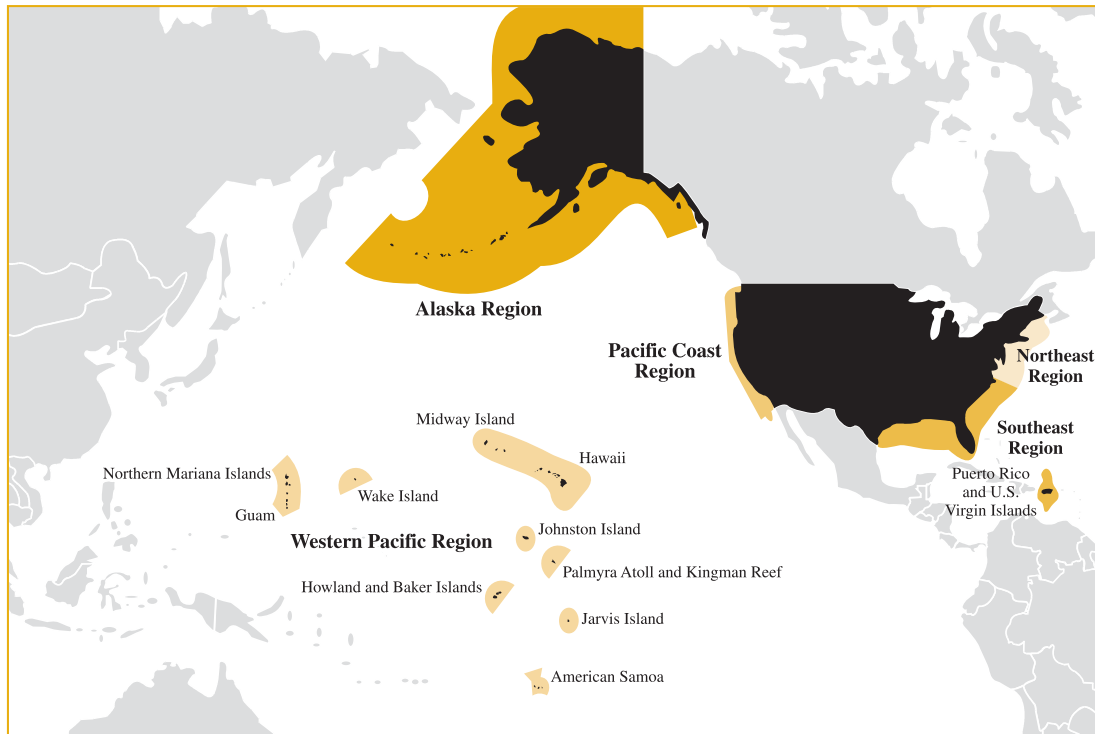
In 2001 GAO identified monitoring and enforcement of trade agreements as a major management issue for Commerce, citing two main reasons for this problem—first, the Department's shortage of staff with the expertise to monitor compliance with trade agreements, and second, its difficulty obtaining balanced, comprehensive input from the private sector.

The Secretary of Commerce has taken steps to address the concerns of both Congress and GAO by making monitoring and enforcing trade agreements a top priority for ITA and for the Department as a whole. Commerce received additional funding for trade compliance activities in FY 2001.

To effectively monitor and enforce trade agreements, ITA must maintain sufficient staff. Currently, we are reviewing ITA's ability to recruit, hire, and retain personnel for selected positions on the Market Access and Compliance staff.

To improve compliance with trade agreements, ITA also needs to promote a more coordinated federal effort. We noted that the bureau's trade agreement compliance process, as managed by the Trade Compliance Center, needs to better coordinate and track trade compliance and market access activities within ITA. The results of this review are described on page 50 of our March 2002 *Semiannual Report to Congress*.

In the future, we intend to review other aspects of ITA's approach to market access and trade compliance, as well as its administra-



The Magnuson-Stevens Act of 1976 established a U.S. exclusive economic zone (EEZ), which ranges between 3 and 200 miles offshore and consists of areas adjoining the territorial sea of the United States, the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and U.S. overseas territories and possessions. NMFS is responsible for conserving and managing the fish, sea turtles, whales, seals, dolphins, and other marine mammals and their habitats within the EEZ.

tion of the antidumping and countervailing duty regulations. In the meantime, ITA must work closely with U.S. companies, other federal agencies, and foreign governments to identify trade compliance problems, develop workable solutions for them, and thus enhance American firms' access to foreign markets.

CHALLENGE 8: INCREASE THE EFFECTIVENESS OF MARINE RESOURCE MANAGEMENT

For nearly 30 years the National Marine Fisheries Service (NMFS) has had to balance two competing interests: promoting commercial and recreational fishing as vital elements of our national economy and preserving populations of fish and other marine life. The Marine Mammal Protection Act of 1972 and the Endangered Species Act of 1973 gave NMFS responsibility for preventing the extinction of marine fish, mammals, and turtles, as well as anadromous fish, such as Pacific salmon, which migrate between the ocean and inland waterways. The Magnuson-Stevens Act of 1976 made NMFS the primary federal agency for

managing marine fisheries and established a regional fishery management system to help the agency carry out its mission. A 1996 amendment to the act strengthened NMFS's role in protecting and sustaining fisheries.

The Department has reported that overfishing and overcapitalization in commercial and recreational fisheries have resulted in estimated losses of billions of dollars in economic growth, thousands of jobs, and countless fishing opportunities. While certain fisheries appear to be well managed and produce positive benefits, others are severely depleted and must be restored and properly managed to realize their long-term potential. At the same time, threatened or endangered fish species need to be replenished. Among 52 distinct groups of Pacific salmon, for example, 26 are threatened or endangered.

NMFS has recently taken steps to restore Pacific salmon runs. In accordance with the Endangered Species Act, the agency's specific responsibility is to manage protected species through conservation programs and recovery plans. Its Federal Columbia River Power System 2000 Biological Opinion and the broader Federal Caucus Basin-wide Salmon Recovery Strategy established performance standards to guide recovery of Pacific salmon

in the Columbia River Basin. NMFS has also put together teams to develop recovery plans for threatened and endangered Pacific salmon species.

OIG recently evaluated the role of NMFS's Northwest Fisheries Science Center in supporting salmon recovery efforts. We focused on the center's implementation of its Salmon Research Plan, which establishes priorities to ensure that the most important scientific work is conducted. While the plan is an important step toward meeting the center's goal of strengthening its salmon research program, we found a number of deficiencies. As a result, we recommended that the center improve its peer review processes, implement comprehensive multiyear plans to measure progress in meeting the goals of the Salmon Research Plan from one year to the next, and develop better procedures for monitoring and evaluating ongoing research and related costs. (See page 32.)

We also completed a review of NMFS's plans to design and construct the first of possibly four acoustically quiet, state-of-the-art fisheries research vessels and found a number of management control weaknesses. For example, the National Oceanic and Atmospheric Administration (NOAA) has not enforced the contract's scheduling requirements, adequately tracked program costs, fully documented the program's management structure, or maintained an official contract file for the acquisition. (Details regarding these and our other findings appear on page 31.)

We are currently evaluating methods used to enforce fisheries management plans. We intend to monitor NOAA's efforts to increase the effectiveness of its marine resource management and will follow up on actions it takes in response to our recommendations regarding the Northwest Fisheries Science Center and the vessel acquisition program.

CHALLENGE 9: CONTINUE TO IMPROVE THE DEPARTMENT'S STRATEGIC PLANNING AND PERFORMANCE MEASUREMENT IN ACCORDANCE WITH THE GOVERNMENT PERFORMANCE AND RESULTS ACT

Congress and agency managers require relevant performance measures and credible performance data to effectively fulfill their oversight responsibilities with respect to federal programs. The Government Performance and Results Act of 1993 was designed to ensure the availability of such data by mandating that agencies

set goals for program performance and report outcomes measured against those goals. As the administration moves toward integrating budget and performance information and using performance data to make funding decisions, the credibility of reported performance results will be critical.

Since 1997 OIG has assessed Commerce's efforts to implement GPRA. To ensure the collection and reporting of accurate, appropriate, reliable, and useful data to decision makers, this office has

- provided implementation advice and assistance,
- monitored reviews by certified public accounting firms of performance data contained in the annual financial statements,
- made presentations to departmental officials on the importance of ensuring that performance-related information is reliable,
- given informal comments to the Department on various GPRA-related documents, and
- audited internal controls for selected data on bureau performance.

Although we believe the Department has made progress toward meeting the challenge of how best to plan and measure its performance, significant opportunities for improvement remain. For one, Commerce should clearly articulate the level of reliability that can be placed on the performance data it provides in its *Annual Program Performance Report* to meet GPRA and other reporting requirements.

Also, our audits of several performance measures used by departmental units (BIS, NIST, NTIA, and USPTO) indicate a widespread need for stronger internal controls to ensure accurate reporting of performance data and improved explanations and disclosures of results. For example, procedures should be established to ensure that (1) reported information is reconciled against supporting data and (2) only data from the appropriate time period is included in performance results.

These issues are again emerging in our current audit of selected performance measures at NOAA. We are concerned that—for the measures we are evaluating—NOAA may need to (1) improve internal controls, (2) restate data that was incorrectly reported in the past, (3) provide additional disclosures and explanations of performance results, and (4) assess the value of certain measures to determine whether they should be dropped, revised, or unchanged.

We will continue to evaluate performance measurement and reporting at NOAA and other bureaus and, as warranted, make recommendations to the Department and its operating units regarding the accuracy, appropriateness, reliability, and usefulness of its performance data.

CHALLENGE 10: EFFECTIVELY MANAGE MAJOR COMMERCE RENOVATION AND CONSTRUCTION PROJECTS

The Department has plans for numerous major³ renovation and construction projects:

- NOAA has 27 projects scheduled or in process. These include modernization of the National Ocean Service’s Marine and Environmental Health Research lab in South Carolina, and a National Marine Fisheries Service lab in Hawaii.
- NIST will continue its multimillion-dollar program to upgrade existing laboratories in Gaithersburg, Maryland, and Boulder, Colorado, and to complete construction of the Advanced Measurement Laboratory building, a new facility in Gaithersburg, Maryland.
- USPTO is implementing its billion-dollar plan to consolidate employees and operations in a new, five-building facility under construction in Alexandria, Virginia (see page 8).
- The Census Bureau intends to construct two buildings at its headquarters in Suitland, Maryland, to provide employees with safe, modern facilities.
- Commerce plans to modernize its headquarters building in Washington, D.C.

Major Construction and Renovation Projects (Current and Planned as of 9/30/02)

Operating Unit	Number of Projects	Estimated Costs (in millions)
NOAA	27	\$558
NIST	2	\$235
USPTO	1	\$1,200
Census Bureau	1	\$340
Office of the Secretary	1	\$360

Note: A project may include more than one building.

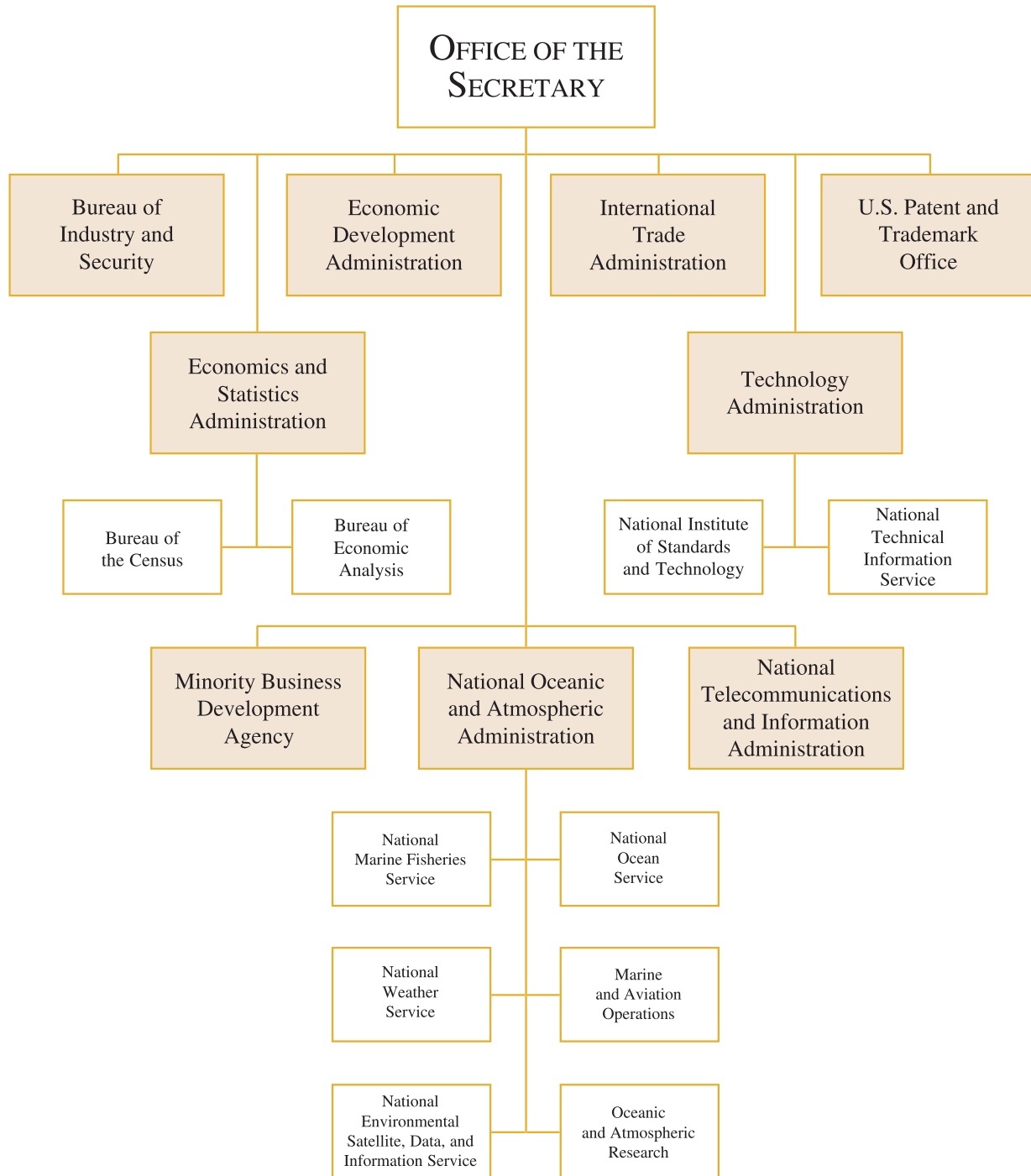
Source: Commerce Office of Real Estate Policy and Major Programs.

Effective renovation and construction management is a critical challenge for the Department because of the numerous inherent risks involved in planning and managing large, costly, and complex capital improvement and construction projects. Departmental leadership and OIG oversight are needed to maximize Commerce’s return on its investment in these projects. Past OIG reviews of major renovation and construction ventures have demonstrated that up-front oversight—that is, close monitoring during planning and implementation—is essential. Detecting and addressing potential problems during the developmental stages rather than after a project is completed save time and money. For this reason, we plan to actively monitor the progress of some of the Department’s current and planned construction projects at Census, NIST, NOAA, USPTO, and other locations as appropriate.

³ Projects costing \$2 million or more are considered major.



Department of Commerce Organization Chart





BUREAU OF INDUSTRY AND SECURITY

The Bureau of Industry and Security

Security is primarily responsible for administering and enforcing the nation's system for controlling exports of sensitive dual-use goods and technologies. BIS's major functions include formulating and implementing export control policy; processing export license applications; conducting various policy, technical, and economic analyses; promulgating regulations; conducting industry outreach; and enforcing the Export Administration Act and regulations. BIS' activities also include promoting federal initiatives and public-private partnerships across industry sectors to protect the nation's critical infrastructures. BIS is divided into two units:

Export Administration implements U.S. export control and nonproliferation laws and policies through export licensing, commodity classifications, and advisory opinions; technical, economic, foreign availability, and policy analyses; promulgation of regulations; and industry outreach. It also conducts various defense industry activities and enforces industry compliance with arms control treaties.

Export Enforcement participates in reviews of export license applications and conducts criminal and administrative investigations relating to the export control portions of the Export Administration Act and regulations. It also administers and enforces the antiboycott provisions of the act and regulations.

SOME KEY RECOMMENDATIONS FROM EXPORT CONTROL REVIEWS REMAIN UNIMPLEMENTED

As required by the National Defense Authorization Act, we conducted our annual follow-up review on the status of recommendations regarding dual-use export controls for which Commerce operating units—principally the Bureau of Industry and Security—are responsible. This year's review looked at recommendations from the three reports we have issued thus far: (1) *Improvements Are Needed in Programs Designed to Protect Against the Transfer of Sensitive Technologies to Countries of Concern* (March 2000), (2) *Management of the Commerce Control List and Related Processes Should Be Improved* (March 2001), and (3) *BXA Needs to Strengthen Its ECASS Modernization Efforts to Ensure Long-Term Success of the Project* (February 2002).

These Department-specific assessments are conducted in addition to the annual interagency reviews we perform with the inspectors general of Defense, Energy, State, and the Treasury in consultation with the directors of the CIA and FBI.

We found that, while BIS has taken action on some of our recommendations, key recommendations from all three reports have yet to be acted on. With the exception of one open item, BIS has responsibility for implementation of the recommendations.

REVIEW RESULTS

March 2000

The focus of our first-year NDAA review was enforcement and implementation of the deemed export regulations,⁴ as well as industry and federal compliance with them; the effectiveness of the Visa Application Review Program; and BIS's success at supporting federal efforts to monitor foreign investment in U.S. companies. We made 24 recommendations to BIS, NOAA, ITA, and NIST for improving programs designed to protect against the transfer of sensitive technologies to countries of concern. Five of our 24 recommendations remain open. Four of these were addressed to BIS, and concern the need to (1) discuss with NOAA the applicability of deemed

⁴ According to the Export Administration Regulations, any release to a foreign national of technology or software subject to the regulations is deemed to be an export to the home country of the foreign national. These exports are commonly referred to as "deemed exports," and may involve the transfer of sensitive technology to foreign visitors or workers at U.S. research laboratories and private companies.

export controls to NOAA’s activities; (2) work with the National Security Council to review the deemed export policy and process; (3) improve the investigative tracking system regarding visa referral information; and (4) periodically assess the visa application review program and develop performance measures to help determine whether resources dedicated to the program are justified.

The remaining open recommendation urged NOAA to establish procedures for ensuring that any technical information or know-how it releases to foreign nationals complies with federal export licensing requirements.

March 2001

We examined BIS’s policies and procedures for the design, maintenance, and application of the Commerce Control List (CCL), which specifies the commodities, software, and technologies subject to Export Administration Regulations. We made 14 recommendations for improving the list and related operations; the bureau has fully implemented only 5. The remaining open items deal with improving various aspects of the CCL, the commodity classification process, commodity jurisdiction determinations, and licensing of night vision technology.

February 2002

Our most recent review assessed BIS’s efforts to modernize its Export Control Automated Support System (ECASS) for dual-use export licensing. We examined whether the bureau had adequately considered life-cycle resources and business process changes; developed a realistic system-design schedule; and established an infrastructure for monitoring costs, schedule, and deliverables. BIS has fully implemented only 4 of our 13 recommendations. Action is still needed to (1) factor into ECASS, as appropriate, changes proposed in the 1998 business process reengineering study and a 2001 internal licensing task force report; (2) determine needed resources, potential funding mecha-

nisms, and feasibility of established time frames; (3) validate systems requirements; (4) document security requirements and calculate associated costs; (5) revise and approve the project management plan; (6) complete target architecture and select a location for ECASS; (7) determine whether the Department of Defense can use ECASS for its licensing needs; (8) work with other licensing agencies to develop a central data repository for records pertaining to reviewed license applications; and (9) develop an interagency agreement that documents the responsibilities and coordination of all dual-use licensing agencies.

PROMPT ACTION NEEDED

Given BIS’s key role in administering the dual-use export control process, we believe the bureau should take quick action to address all of the open recommendations.

Status of OIG Recommendations

Fiscal Year	Number of Recommendations	Number Closed
2000	24*	19
2001	14	5
2002	13	4

* Combined number of recommendations made in our March 2000 report on programs designed to protect against transfer of sensitive technologies to countries of concern, made to BIS, NOAA, ITA, and NIST.

In addition, we asked BIS to look into our concerns about the adequacy of export license application review by one of the other federal agencies involved in the process and to open discussions with that agency about its limited analysis of license applications. *(OFFICE OF INSPECTIONS AND EVALUATIONS: IPE-15290)*



ECONOMIC DEVELOPMENT ADMINISTRATION

The Economic Development Administration

Administration was established by the Public Works and Economic Development Act of 1965 to generate new jobs, help retain existing jobs, and stimulate commercial and industrial growth in economically distressed areas of the United States. EDA continues to fulfill this mission under the authority of the Economic Development Administration Reform Act of 1998, which introduced the concept of Comprehensive Economic Development Strategies, a local planning process designed to guide the economic growth of an area. Based on these locally and regionally developed strategies, EDA works in partnership with state and local governments, regional economic development districts, public and private nonprofit organizations, and Indian tribes to help distressed communities address problems associated with long-term economic deterioration and recent, severe economic dislocations, including recovery from the economic impact of natural disasters, the closure of military installations and other federal facilities, changes in trade patterns, and the depletion of natural resources. EDA provides eligible recipients with technical assistance, as well as grants for public works and economic development, planning, training and research, and economic adjustment.

EDA helps American businesses generate employment and America's communities weather adverse economic events or trends. To fulfill its mission, EDA has developed eight assistance programs, which it refers to as "investment programs," that provide financial assistance through grants to state and local governments and nonprofit economic development organizations. The monies are used to fund such efforts as economic development planning, public works projects, and revolving loan funds.

EDA Assistance Programs

- Public Works Program
- Economic Adjustment Program
- Research and National Technical Assistance Program
- Partnership Planning for Economic Development Districts, Indian Tribes, and Other Eligible Areas
- Short-Term Planning to States, Sub-State Planning Regions, and Urban Areas
- Technical Assistance Program (Local)
- University Center Program
- Trade Adjustment Assistance Program

REVOLVING LOAN FUNDS

EDA's Economic Adjustment Program provides, among other things, grants to capitalize revolving loan funds (RLFs). As of September 30, 2002, there were 611 RLFs with a total of \$550 million in federal funds. The program focuses on communities and regions that have experienced or are threatened by serious structural damage to their underlying economic base. RLFs offer loans to local businesses that otherwise cannot secure sufficient private financing. During this semiannual period we completed audits of 9 revolving loan funds, several done at the request of EDA, and found that of these, 6 have excess cash reserves resulting from lack of demand for loans and 8 committed significant violations of program regulations including mismanagement of funds. Recommendations to correct these problems involve \$9.2 million in funds that could be put to better use. EDA management has been active in implementing our recommendations.

AUDIT PREVENTS INELIGIBLE LOANS BEING MADE IN OKLAHOMA

In February 1999 an Oklahoma development district received a \$350,000 Long-Term Economic Development (LTED) grant to capitalize a revolving loan fund. The grant agreement required the district to provide a \$117,000 matching share, which brought the RLF's total capitalization to \$467,000. Like other RLF grant agreements, it also required that the recipient meet grant disbursement milestones.

During our September 2001 audit of the RLF (ATL-14301-1) to determine why the district had not drawn down any of the grant funds, we found that the lack of funds usage (therefore, failure to meet RLF disbursement milestones) resulted from a lack of demand for RLF program loans. We recommended, therefore, that EDA terminate the award and deobligate the grant funds. EDA concurred and complied with our recommendations.

The district, however, appealed the agency's decision, stating that it had approved two loans at about the time EDA terminated the grant and claimed that the RLF was legally obligated to fund the loans. EDA's appeal decision instructed the district to provide a legal opinion that the two loan commitments were legally binding and certify that the loans were made in compliance with program requirements. The decision also provided for an OIG audit of the two loan applications. We conducted our audit in May 2002 and determined that neither application was in compliance with RLF requirements, which generally do not permit loans to borrowers who can obtain financing from private lenders, because both applicants were eligible to obtain private funding. In fact, one borrower had been offered a loan with an 8.5 percent interest rate from a local bank but accepted the RLF loan because its interest rate was 6 percent. The second borrower applied for funding to expand his company but was shown during our audit to have already obtained alternative financing.

Based on our findings, we recommended that EDA neither obligate nor disburse the \$300,000 federal share requested by the district to fund the two loans. While it disagreed with our interpretation of program requirements, the district concurred with our audit findings, as did EDA. Implementing our recommendation will allow \$300,000 in EDA funds to be put to better use. (*ATLANTA REGIONAL OFFICE OF AUDITS: ATL-14301-2*)

TERMINATION FOR CAUSE PROMPTED BY GROSS MISMANAGEMENT OF OHIO LTED GRANT

At EDA's request we performed an audit of an RLF established in 1980 through a \$400,000 LTED grant awarded to an Ohio city. Our objective was to determine the fund's current assets so that EDA could terminate the award and recoup the fund balance.

The audit, conducted in February 2002, was our second examination of this RLF. The first, conducted in 1991, revealed management and compliance deficiencies so serious that we recommended EDA phase out the grant and obtain repayment of the RLF balance—\$178,769 (DEN-0298). EDA concurred with these recommendations, but has since been unable to obtain either the balance or the documents needed to terminate the grant.

In November 2001 EDA asked the city to calculate the current dollar value of the RLF so that termination could be finalized, but the city claimed it was unable to do so. EDA then asked us to determine the RLF balance due.

City failed to account for RLF assets

Our audit found that the city failed to maintain adequate records to account for RLF principal, interest earned, loan repayments, and other financial aspects of the EDA award. The RLF agreement obligated the city to submit semiannual reports to EDA, but it had not done so for a decade. Its last report, issued in 1992, revealed total RLF assets of \$335,540: \$47,002 in cash and \$288,538 in outstanding loans. During our 2002 audit we found that the city had two accounts relating to the RLF with combined assets of \$216,570 as of December 31, 2001. However, we had no basis to conclude that the balances in these accounts accurately reflected the current RLF balance because the city was unable to provide us with any transaction histories to allow us to determine whether loan repayments and interest were properly credited or whether any inappropriate withdrawals had been made.

City failed to adequately pursue defaulted loans

In 1992 the city reported three defaulted loans totaling \$62,307 and three current loans for \$226,231. Our review of the 1992 loan files indicated that the city did not adequately pursue collection on the defaulted loans. Of the then-current loans, one has since been paid in full and the other two are in default. Two of the defaulted borrowers, who together owe the RLF more than \$140,000, still operate the businesses for which the loans were made. Although the city appeared to make some initial collection efforts in 1993, there was no information in loan files to document whether attempts have been exhausted or collections made. Because the city neglected its obligations under the RLF award by failing to pursue collection in a prudent and timely manner, we have held the city accountable for the total amount of the defaulted loans in computing the value of the RLF.

Fund administrator improperly borrowed \$38,223 from the RLF

We found that between 1991 and 1993, the city improperly allowed its loan administrator to borrow \$38,223 from the RLF to continue operations over a 2-year period, and there was no evidence of repayment. We therefore determined that the city should be held accountable for the amount borrowed, which was included in the cash asset total we used to calculate monies due to EDA.

\$513,480 due to EDA on termination of the RLF

When a recipient fails to comply with the conditions of an RLF grant and fails in its fiduciary responsibilities as trustee, EDA may terminate the grant for cause and recover its fair share of the RLF's value. Due to the seriousness and persistence of the city's compliance failures, we recommended that EDA take immediate action to terminate the grant and obtain reimbursement for the current value of the RLF, which we calculated to be \$513,480, based on the 1992 fund balance of \$335,540 plus imputed interest of \$177,940 as of December 31, 2001. EDA concurred with our recommendations. (*DENVER REGIONAL OFFICE OF AUDITS: DEN-14962*)

NEW YORK RLF MAINTAINED EXCESS CASH RESERVES FOR 11 YEARS

In September 1979 EDA awarded a \$2,223,000 LTED grant to a city in New York to establish an RLF. One year later the award was amended to add \$1,777,000, increasing the RLF's capitalization to \$4 million. In May 1997 EDA approved the city's request to amend the grant agreement, allowing the city to use RLF funds to make loan guarantees.

At EDA's request we performed a financial and compliance audit during April 2002 to determine (1) the financial status of the RLF; (2) the city's compliance with applicable federal laws and regulations, and terms and conditions of the grant; and (3) whether specific administrative costs charged to the RLF were allowable.

Our audit disclosed that the fund had \$2,375,749 in excess cash as of March 2002 and had maintained excess funds for at least 11 years, in violation of EDA guidelines and RLF program objectives. The excess resulted from the city's prolonged low level of RLF activity: the city ceased making loans in early 1994, and only five loan guarantees have been made since 1997. Although the city has recently identified several opportunities for rejuvenating the program, we recommended that EDA require the city to

- deposit the \$2,375,749 in excess funds into a separate, interest-bearing account and remit the interest monthly to the U.S. Treasury;
- use the excess funds within 6 months to make direct loans or loan guarantees in accordance with RLF program objectives; and
- remit unused excess funds in the account after 6 months to the U.S. Treasury.

Our audit also disclosed that the city was not in compliance with several RLF administrative requirements regarding submission of mandated RLF status reports and annual plan certifications to EDA. In addition, \$57,977 in unsupported administrative costs was charged to the RLF during the audit period. To correct the administrative findings, we recommended that EDA require the city to submit annual RLF plan certifications, ensure that semi-annual status reports are accurate and timely, and reimburse the fund for \$57,977 in unsupported administrative costs.

City officials agreed with the audit findings, noting that our recommendations either have been or would soon be implemented. (*ATLANTA REGIONAL OFFICE OF AUDITS: ATL-15125*)

ARKANSAS DISTRICT CITED FOR UNALLOWABLE LOANS, UNCOLLECTED DEBT, AND UNSUBMITTED DOCUMENTATION

In 1978 an Arkansas economic development district received a \$720,000 Economic Adjustment Assistance grant to establish a revolving loan fund with which to implement a comprehensive economic adjustment program for nine Arkansas counties. No local match was required.

Our audit, conducted during April 2002, evaluated the district's financial management of the RLF and its compliance with applicable administrative requirements. Based on our examination of 16 loans active as of September 30, 2001, the following instances of noncompliance were found:

- From 1992 through 2001 the district awarded 16 loans; 12 of them had a \$264,000 leverage shortfall. For the remaining 4, although \$565,000 was proposed as leverage, the district did not confirm \$294,000 of the proposed amount.
- The district awarded three loans totaling \$140,000 to refinance existing debt, a use program requirements generally prohibit. (Certain limited exceptions apply, but they must be properly documented.) In addition, one of the loans was in default.
- The district failed to comply with the EDA requirement that sound management procedures be used to collect payments on RLF loans. Six loans awarded to five borrowers from 1992 through 1999 lingered in long-term default, with outstanding balances totaling \$221,247 and past due interest totaling \$93,707. Two loans to one borrower had been in default since October 1993, with outstanding balances totaling \$109,569 and past due interest totaling \$61,178; yet the district had failed to take action to collect on the loans.

RLF Grants Improperly Awarded to Refinance Existing Debt (for period ending September 30, 2001)

Borrower	Loan Amount	Balance
1	\$ 50,000	\$ 40,036*
2	10,000	6,236
3	80,000	79,709
Totals	\$140,000	\$125,981

*Loan in default at time of OIG audit.

RLF Loans in Default (for period ending September 30, 2001)

Borrower	Loan Amount	Past Due Interest	Principal Balance
1	\$100,000	\$50,473	\$ 94,569
2	15,000	10,705	15,000
3	50,000	6,240	40,036
6	25,000	6,597	22,974
5	30,000	11,877	28,668
6	20,000	7,815	20,000
Totals	\$240,000	\$93,707	\$221,247

Note: Borrowers #1 and #2 are the same company.

- From October 1, 1995, until September 20, 2001, the district did not submit required financial reports.
- The district did not have written procedures or proper documentation for monitoring and servicing RLF loans, as required by EDA. Its loan files consistently lacked, among other things,
 - loan applications and committee approvals;
 - evidence of leveraging or borrower equity, or insurance;
 - credit checks and verification of funds used as intended; and
 - records of correspondence with the defaulted borrower.

We recommended that EDA require the district to (1) recall \$85,945 in outstanding balances on the two loans made to refinance existing debt; (2) confirm leveraging of \$294,000 for two RLF borrowers and ensure that future loans are properly leveraged; (3) pursue collection of \$221,247 for six defaulted loans

and \$93,707 for past due interest; (4) submit annual reports to EDA in a timely manner; and (5) submit a revised RLF plan that includes written procedures for monitoring and servicing its RLF loans and handling defaulted loans. (DENVER REGIONAL OFFICE OF AUDITS: DEN-15019)



Lack of written documentation (for example, proof of fire insurance) increases the risk that RLF funds are not being administered in accordance with EDA regulations, placing federal funds at risk.

EXCESS CASH RESERVES, IMPROPER CLAIMS, AND NONCOMPLIANT INDEPENDENT AUDITS FOR MICHIGAN RLF

In 1979 a Michigan city received a \$4.85 million LTED grant: \$1.8 million as a direct loan and \$3.05 million for a land write-down program.⁵ In 1980 EDA transferred \$1 million from the write-down program to the city to establish an RLF to address major industrial dislocations and consequent unemployment. (EDA terminated the program’s remaining \$2.05 million in 1983.) In 1988 \$600,000 of an EDA RLF grant to the state of Michigan was transferred to the city. Thus the RLF’s total capitalization was \$1.6 million.

As of September 2001, the city reported having made 80 loans: 61 had been fully repaid, 14 were active, and 5 written off. Income earned on the RLF had increased its capital balance to

⁵ Land write-down: A subsidy offered when a development authority acquires a property and sells/transfers it to a private developer for less than the acquisition price as an incentive for business development. Example: if a city sells a cleared land parcel to the developer for \$1 instead of the assessed value of \$200,000, then the developer would have received a subsidy of \$199,999 over what was required to enable the project to proceed.

about \$2.9 million—\$913,441 in outstanding loans and \$2,023,720 in cash.

We audited the RLF in February 2002 to evaluate the city’s financial management of the fund and its compliance with administrative and loan documentation requirements. Our audit disclosed excess cash reserves, improper administrative charges, and inadequate audit coverage.

\$749,430 in excess cash reserves

The city’s capital utilization rate for September 2001 was 49 percent—far less than EDA’s required 75 percent utilization. The 14 active loans represented an outstanding principal balance of \$913,441, and \$540,000 was recorded against loan commitments, for a total capital utilization of \$1,453,441. This left \$1,483,720 available for new loans, more than twice as much as the 25 percent reserve permitted by EDA.

RLF Financial Status as of September 2001

RLF capital base	\$2,937,161
Capital utilization	-1,453,441
Available for new loans	= \$1,483,720
Cash balance allowed by EDA	-734,290
Excess Cash Reserves	= \$ 749,430

The city agreed with our finding of excess cash reserves but requested that EDA delay implementing our recommendation until after its September 2002 semiannual report, claiming that all excess cash reserves were currently earmarked for loans: \$440,000 currently approved but not yet disbursed and applications totaling \$900,000 awaiting review. Under the circumstances, we recommended that EDA require the city to sequester any excess cash reserves as of September 30, 2002, in an interest-bearing account and remit interest earned on the account to the U.S. Treasury.

\$197,323 in improper administrative expenses

Administrative costs claimed, totaling \$197,323, were improperly based on a percentage of the RLF’s interest income rather than actual costs incurred. Although the city maintained meticulous loan files and the claimed expenses appear low compared to the actual costs required to administer the program, the lack of documentation for costs claimed is not justified.

The city agreed and subsequently provided documentation that the claimed amount actually had been incurred. It also stated that—as we had recommended—it had revised its accounting system to record administrative costs in the general ledger. In our final report we recommended that EDA ensure that the city’s administrative cost claims are based on actual expenses incurred, not estimates. EDA concurred.

Independent audits lacked required disclosures

The city’s annual audits were not conducted in accordance with OMB Circular A-133, as required by the terms and conditions of the EDA grant, and therefore excluded EDA-required disclosures such as a schedule of federal assistance and reports on internal controls and compliance with laws and regulations.

We recommended that EDA require the city to obtain annual audits that comply with OMB Circular A-133. The city stated that it was unaware of its noncompliance and agreed to obtain the required audits for all future periods. *(DENVER REGIONAL OFFICE OF AUDITS: DEN-14963)*

U.S. VIRGIN ISLANDS AUDIT DISCLOSES ADMINISTRATIVE, FINANCIAL, AND REPORTING PROBLEMS

An economic development agency in the U.S. Virgin Islands administers two EDA revolving loan funds. The first, established in 1986 with a Sudden and Severe Economic Dislocation (SSED) grant of \$300,000 and a recipient match of \$100,000, was created to provide needed financing for new and existing businesses in economically depressed areas of the islands. The second, established in 1990 with a \$500,000 award, was provided to assist businesses adversely affected by Hurricane Hugo. As of March 2002 the RLFs had made 34 loans totaling \$1.3 million; however, no loans from either fund had been made since 1994.

At the request of EDA, in April 2002 we conducted an audit to determine the financial status of the two RLFs and the recipient’s compliance with applicable federal laws and regulations, EDA grant terms and conditions, and RLF plans. Our audit uncovered numerous problems with the administration and financial management of the RLFs:

- The recipient’s accounting records were inadequate and did not support the cash balance it reported for the two RLFs (roughly \$971,000).
- Contrary to EDA requirements for the revolving loan

fund program, the RLFs carried excess cash reserves for 3 consecutive years. At the time of our audit the excess cash balance was \$576,000.

- Of the 34 loans made, 17, totaling \$617,000 (99 percent of outstanding principal), were in default. Of that 17, 5 had been in default for more than 8 years; 11 were made to companies that have since gone out of business; 3 were made despite the loan officer's recommendations that they be denied; and 1, because it was made to a legislator, created the appearance of conflict of interest.

Our audit also disclosed that the recipient regularly failed to meet RLF reporting requirements, and there was no evidence that annual RLF plan certifications were ever prepared.

To ensure that the RLF is properly managed and accounted for in the future, we recommended that EDA require the recipient to implement sound lending practices to manage the RLF portfolio and include specific audit procedures in its annual operational audit under the Single Audit Act. We also recommended that the recipient be directed to return \$499,680—the agency's share of excess RLF cash—to the U.S. Treasury.

The recipient agreed with our findings regarding mismanagement of the RLF, but noted that the problems had occurred under a previous administrator and pledged to improve operations in the future. (*ATLANTA REGIONAL OFFICE OF AUDITS: ATL-15126*)

LACK OF LOAN ACTIVITY FUELS ACCUMULATION OF \$1.5 MILLION IN EXCESS CASH RESERVES FOR WISCONSIN RLF

In September 1985 EDA awarded an \$800,000 LTED grant to a city in Wisconsin to establish a revolving loan fund that—with the city's required match of \$400,000—was capitalized at \$1.2 million. The RLF targeted a part of the city plagued with long-standing economic distress and high rates of unemployment and business failure. Its purpose was to fund small business expansion and create jobs to replace those lost from business closures or relocations. The RLF is administered by a local development corporation that operates a total of six funds for the city. As of September 30, 2001, the RLF had total assets of \$2,153,000—\$2,030,876 in cash and \$122,124 in outstanding loans.

We performed our audit in December 2001 to evaluate the financial management of the RLF and the grantee's compliance with applicable RLF administrative requirements. We found that the city was not making use of the fund—the outstanding loan

amount represented only 6 percent of the RLF's available funding rather than the 75 percent utilization rate required by EDA—and no loans had been made in 6 of the last 7 years. In the meantime the fund had been accumulating substantial excess cash reserves and the cash balance had grown by more than \$600,000 in the prior 4 years.

In May 2001 the grantee requested that EDA allow expansion of the RLF project area to include the entire city. However, the city is already served by two non-EDA revolving loan funds that together have some \$41 million available for lending. EDA's grant terms and conditions require that its RLF awards not duplicate programs funded by other sources; therefore we recommended that the agency review the city's request to ensure that it will not duplicate existing loan programs.

We also recommended that EDA require the city to immediately sequester the RLF's \$1.5 million excess cash balance in a separate, interest-bearing account and remit the interest to the U.S. Treasury. (*DENVER REGIONAL OFFICE OF AUDITS: DEN-14885*)

FOLLOW-UP OF 1994 AUDIT REVEALS OLD AND NEW PROBLEMS WITH ARKANSAS RLF

A planning and development district in east Arkansas received an LTED grant for \$500,000 in September 1982 to establish a revolving loan fund. Over the years, EDA twice amended the original grant, ultimately increasing the federal share to \$2,011,747. With a district match of \$136,402, total RLF capitalization amounted to \$2,148,149.

In 1994 we audited the RLF to assess the district's financial management and compliance with EDA's administrative requirements. We found the district's handling of the RLF was noncompliant in several respects. Specifically, the recipient maintained excess cash balances in the RLF, and insufficient loan documentation and inadequate accounting systems exacerbated the likelihood of loan losses.

During this semiannual period our follow-up audit of the Arkansas RLF program disclosed that not only had the district failed to correct the deficiencies we previously noted but further mismanagement was evident. The district continues to carry excess cash reserves and lacks proper loan procedures and documentation. The district also (1) inappropriately used RLF funds to refinance existing debt, (2) had a leverage shortfall for nine loans, (3) did not confirm millions of dollars in leverage claims, and (4) did not actively pursue collection of defaulted loans. In addition, the district provided inaccurate semiannual reports to

EDA, including a September 2001 report that overstated the RLF's cash balance by \$1.7 million.

Evidence of Mismanagement Disclosed by 2002 Audit

Noncompliance	Number of Loans	Amount
Refinanced debt	7	\$679,718
Leverage shortfall	9	\$391,335
Unconfirmed leverage	24	\$5,000,000
Unpursued defaulted loans	7	\$154,792

We recommended that EDA require the district to take the following actions:

1. Return \$147,490 in excess cash reserves to EDA.
2. Recall \$505,947 in outstanding debt on the seven ineligible loans that were made to refinance preexisting debt.
3. Confirm leveraging of \$5 million for 24 RLF borrowers and ensure that future loans are leveraged adequately.
4. Pursue defaulters for collection of principal and past due interest.
5. Work with its accounting firm to ensure that its semiannual reports are accurate and reconcile to RLF financial statements.
6. Revise its RLF plan to specify written procedures for monitoring and servicing loans, handling defaults, producing accurate reports, and maintaining required loan documentation.

The district agreed to return the excess cash reserves to the government. (DENVER REGIONAL OFFICE OF AUDITS: DEN-14884)

AUDIT OF PENNSYLVANIA RLF DISCLOSES EXCESS CASH AND FINANCIAL MANAGEMENT ISSUES

The closing of three U.S. Navy facilities in eastern Pennsylvania prompted EDA to award a \$2.7 million Sudden and Severe Economic Dislocation grant to a local industrial development authority in April 1993. The grant included \$1.6 million to establish a revolving loan fund and required the

authority to provide a \$750,000 match. The RLF was established to assist defense-dependent businesses convert to non-defense-related ventures and to help other businesses create new jobs for dislocated workers.

We performed an audit during April 2002 to determine (1) the financial status of the RLF, (2) the fund administrator's compliance with applicable laws and regulations as well as with the terms and conditions of both the EDA grant and the RLF plan, and (3) the propriety of administrative costs charged to the RLF.

Our audit disclosed that the RLF had \$735,048 in excess cash as of March 2002 and had retained excess funds for three consecutive semiannual periods, contrary to EDA guidelines and RLF program objectives. The excess exists because the grantee has not made enough new loans in recent years to expend revenue generated by loan repayments and investment income.

In response to our draft report, the development authority advised us that a recent amendment to its RLF plan would allow it to lend up to \$1.31 million to a local firm for a term of 15 years, thereby eliminating the excess cash balance. While we acknowledge that the amendment provides the RLF the authority to make this previously undisclosed loan, we are concerned about its high dollar value and lengthy term, as well as the fortuitous timing of the proposed transaction. Accordingly, if the loan is approved, we plan to conduct a follow-up audit to determine whether it complies with all applicable RLF eligibility requirements. Otherwise, our initial recommendation—that EDA recoup the \$500,458 federal share of the excess cash—should be promptly implemented.

Additional Findings

Our audit also disclosed that the fund administrator has not complied with certain other RLF administrative requirements. Specifically, it did not record \$16,410 in RLF loan fees as income or deposit this income into the RLF account and did not submit required RLF status reports to EDA for three consecutive semiannual periods. Additionally, the grantee has not submitted required annual RLF plan certifications to EDA and erroneously charged \$4,875 in administrative costs to the RLF.

The administrator has since deposited the \$16,410 to the RLF account and reimbursed the fund for the \$4,875 in incorrect administrative charges. To correct the other deficiencies, we recommended that EDA direct the grantee to submit annual RLF plan certifications and RLF status reports that are complete, accurate, and on time. (ATLANTA REGIONAL OFFICE OF AUDITS: ATL-15123)

PUBLIC WORKS PROGRAM

The Public Works Program (PWP) empowers distressed communities in economic decline to revitalize, expand, and upgrade their physical infrastructure to attract new industry, encourage business expansion, diversify local economies, and generate or retain long-term, private sector jobs and investment. In many cases, Public Works Program projects are used to upgrade or expand an area's economic infrastructure to support the next generation of industry or commerce. Whenever possible, this program seeks to redevelop existing facilities and industrial/commercial locations. EDA encourages such redevelopment projects because they promote sustainable economic development by taking advantage of readily available infrastructure and markets. During this reporting period we audited two PWP grants resulting in recommendations involving \$1.1 million that could be put to better use and \$98,000 in questioned costs.

DUPLICATE FUNDING JUST ONE OF SEVERAL ISSUES REVEALED IN AUDIT OF WASHINGTON ROAD PROJECT

In August 1997 EDA awarded a public works grant to a city in Washington State for construction of a two-way access ramp extending from a bridge, over railroad tracks near the city's marine terminals, and connecting to an existing roadway system. The project, which also included construction of several surface streets,⁶ was intended to improve access to a proposed 29-acre industrial campus of a major pharmaceutical company. The enhancements would also relieve vehicle congestion and improve traffic flow in the area.

Total estimated cost of the project was \$12.5 million, of which the EDA grant would cover \$3 million and the city and other local contributors would provide \$9.5 million. By late 2001 the city had substantially completed the construction project, but EDA had not yet disbursed any of the grant funds. In addition, the city had exceeded the approved EDA budget by about \$6.4 million, with the bulk of the overrun (nearly \$5.3 million) attributable to land and right-of-way expenditures, which had been greatly underestimated in the original budget proposal.

We performed an audit to determine why no EDA funds had been disbursed and whether the grantee's financial management systems complied with federal and EDA requirements. We found

⁶ A surface street allows access by traffic signal or stop sign or allows turns across opposing traffic, as opposed to a freeway where access is provided only by ramps and merges, with no stopping or turning across opposing traffic.



Picture of the "flyover" road (two-way access ramp) built above railroad tracks near the marine terminals.

that no funds had been disbursed because the city had yet to submit any cost claims against the grant. However, it had submitted claims against—and received reimbursement from—a \$10.3 million U.S. Department of Transportation grant it obtained through the state transportation department for essentially the same purpose as the EDA award. We found the city's performance under the terms of the EDA grant agreement to be deficient in several respects.

First, the city failed to notify EDA of the DOT grant, despite the award's terms and conditions requiring such notification. City officials reported that they sought the additional funding after estimates of the project's costs were revised upward (final costs were \$18.3 million). Although they contended that the EDA project manager knew of the DOT award, they could not supply documentation showing that they had formally notified the agency. We recommended that EDA amend its award agreement to reflect the additional project costs and funding.

Second, in meeting its cost-sharing requirement for the DOT grant, the city counted costs that were applicable to its matching share under the EDA grant. In accordance with federal regulations, we recommended that EDA accept for reimbursement only those allowable costs that had not been already claimed against the DOT grant.

City officials generally agreed with our audit findings and are working with EDA to address our concerns and recommendations. (*SEATTLE REGIONAL OFFICE OF AUDITS: STL-14837*)

PROBLEMS WITH CALIFORNIA PROJECT'S EDA AWARD MIMIC THOSE FOUND IN ITS MBDA PROGRAM

A southern California transportation authority representing a consortium of cities is conducting a \$2.4 billion public infrastructure improvement project to consolidate four access rail lines serving two major ports into a single, rail-cargo expressway that links the ports to transcontinental rail yards 20 miles away. In 1996 EDA awarded to the lead city the first of five grants to fund a business outreach program designed to help minority, female, and disadvantaged enterprises secure 22 percent of contract dollars awarded by contractors building the transportation corridor. The program is currently operating under the fifth award.

The initial grant and follow-ons have been administered by the city's Minority Business Opportunity Committee (MBOC), a component of the mayor's Office of Economic Development. This is the same organization that operates another Commerce-funded program through a cooperative agreement from MBDA (see page 28).

We conducted an audit of three of the grants to determine whether the recipient was achieving award objectives; claiming reasonable, allowable, and allocable costs; and complying with federal requirements and grant terms and conditions. Many of the problems we uncovered are closely related to those we found during our audit of the city's MBDA-funded program.

Summary of findings

We found that the recipient consistently met its program objectives for the period under audit. It failed, however, to implement key management controls for procurement and financial management systems.

Procurement. The city could not document the methods used to acquire consulting services and establish compensa-

tion rates. Also, it awarded several personal services contracts to the consultant serving as MBOC director to simultaneously head the EDA grant project. We concluded that the consulting agreements were not competitively awarded and duplicated other agreements the city had with this same consultant. In addition the city could not demonstrate the reasonableness of the compensation in any of the duplicative agreements; and the contracts for these services were unclear and inconsistent in estimates of time, effort, and rate of payment. They also omitted federally required contract clauses.

Financial management. The city could not adequately document time and labor expenses charged to the grants and failed to apply proper rates for fringe benefits and indirect costs.

Recommendations

Taken together, the procurement and financial management failings weakened the recipient's control over the project and the federal funds, leading us to question nearly a quarter of the costs claimed against the three EDA grants and to recommend that EDA take the following actions:

1. Disallow \$215,868 in questioned costs and recover the federal share—\$97,897.
2. Advise the recipient that no costs claimed under the personal services contracts for the project director are allowable for EDA participation.
3. Review the personal services contract currently in force and a schedule of payments made and claimed under the ongoing award and determine whether the conditions we noted in our audit continue.
4. Given that the corridor project is nearing completion, require the recipient to justify a continued need for a project director. If one is needed, require the recipient to demonstrate full compliance with minimum federal procurement standards.

Summary of Grants under Audit

Grant	Award Period	Federal Rate (%)	Federal Share Not-to-Exceed	Local Share	Total Estimated Project Cost
A	02/01/98 - 09/30/99	68.3	\$220,000	\$102,011	\$322,011
B	05/01/99 - 06/14/00	46.4	99,999	115,724	215,723
C	06/15/00 - 12/31/01	38.3	150,000	241,953	391,953
Totals			\$469,999	\$459,688	\$929,687

5. Confirm that the recipient is now completing required certifications and utilizing city time sheets to support time and labor charges, and ensure that approved rates for fringe benefits and indirect costs are being correctly applied.

Interagency funding issues

Because the financial and compliance deficiencies we found in this audit parallel those identified in our audit of the MBDA cooperative agreement, we also recommended that EDA coordinate with the Department's grants officer and MBDA to resolve findings common to both. (*SEATTLE REGIONAL OFFICE OF AUDITS: STL-14900-2*)



ECONOMICS AND STATISTICS ADMINISTRATION

CENSUS LESSONS LEARNED

The **Economics and Statistics Administration** analyzes economic developments, formulates policy options, and produces a major share of U.S. government economic and demographic statistics. The Chief Economist monitors and analyzes economic developments and directs studies that have a bearing on the formulation of economic policy. ESA has two principal agencies:

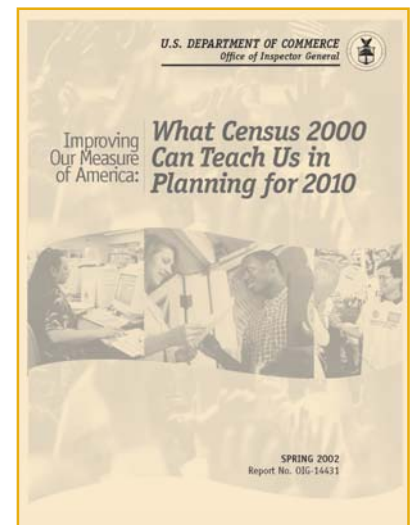
Bureau of the Census is the country's preeminent statistical collection and dissemination agency. It publishes a wide variety of statistical data about the nation's people and economy, conducting approximately 200 annual surveys, in addition to the decennial census of the U.S. population and the decennial census of industry.

Bureau of Economic Analysis prepares, develops, and interprets the national income and product accounts (summarized by the gross domestic product), as well as aggregate measures of international, regional, and state economic activity.

ESA's Bureau of the Census conducts some of the most important work of our nation—taking the measure of America through tabulations of population, economic, geographic, education, housing, and other statistics. In our March 2002 semiannual report, we featured a special report, *Improving Our Measure of America: What Census 2000 Can Teach Us in Planning for 2010* (Report No. OIG-14431). That report summarizes the findings of a decade of monitoring, evaluating, and reporting on the work of the 2000 decennial census. The report offers insights intended to help the bureau capitalize on its successes, improve areas of weakness, and anticipate emerging challenges as it plans for Census 2010; the essentials of these insights have been condensed into 10 lessons learned:

1. Reach early consensus on the 2010 design to facilitate effective planning and obtain sufficient funding.
2. Produce accurate, complete address lists and maps.
3. Conduct a carefully targeted and aggressive public awareness campaign.
4. Strengthen quality control of nonresponse follow-up.
5. Implement clear policies and guidance for managing temporary staff.
6. Determine whether sampling has a role beyond measuring coverage.
7. Implement rigorous system and software development processes and effective information security measures.
8. Upgrade and maintain contracting and program management expertise.
9. Generate timely, accurate management and operational information.
10. Mitigate potential disruptions and distractions to the work environment and workforce.

During the 2000 decennial, the Census Bureau delivered 117 million questionnaires to houses, apartments, mobile homes, and other sites. Recipients were asked to complete a questionnaire for their household and mail it back to the bureau. For households that did not receive a mailed questionnaire or did not return the form, the bureau conducted nonresponse follow-up (NRFU)—dispatching enumerators to personally contact residents and obtain questionnaire information. When enumerators were unable to contact the occupant of a unit, they were to gather “proxy” information from knowledgeable neighbors under very specific Census guidelines. But proxy information tends to be incomplete and less reliable than information received from an occupant of the household. Also, high percentages of questionnaires containing proxy-provided data indicates that enumerators were having problems collecting the necessary data.



Quality data is critical to the integrity of the entire census. Problems with data quality and quality control, when prevalent and when identified while NRFU operations are still in progress, can lead to large-scale reenumerations such as occurred in three Florida counties.⁷

ALLEGED DATA FALSIFICATION IN PHILADELPHIA UNDERScores IMPORTANCE OF QUALITY CONTROL

During this last semiannual period, we completed our review of nonresponse follow-up operations in the North Philadelphia Local Census Office. The purpose of our review was to examine allegations that, to complete nonresponse follow-up on time, some enumerators at that office falsified data included on Census questionnaires. Because NRFU operations had concluded and the office was closed, we were unable to determine the validity of the charges. Nevertheless, we informed the bureau of the allegations and asked that it evaluate the Philadelphia office's nonresponse follow-up data collected during the latter phase of the operation. Upon completing its review, the bureau informed us that it believed the quality of the data was satisfactory overall. But this situation again highlights the importance of, and need for, the bureau to strengthen quality control of nonresponse follow-up, number 4 in our list of lessons learned.

In our review of this situation, we also sought to determine whether enumerators complied with Census Bureau procedures for collecting data and performing quality control checks; we found several conditions regarding data quality and quality control. Some enumerators did not follow prescribed procedures regarding the number of attempts to make to collect information from occupants, and they arbitrarily used proxies when making

personal visits. Also, the number of suspect questionnaires we examined indicated that crew leaders, too, failed to follow procedures. In addition, reinterviewers did not follow procedures when reviewing questionnaires for completeness and accuracy. We believe these findings warrant the bureau's attention. In this and previous OIG reports, we highlighted actions the bureau needs to consider to better ensure data quality and control for Census 2010:

- Continue to select a sample of questionnaires for reinterview throughout nonresponse follow-up.
- Improve local offices' handling of reinterview forms to ensure that selected questionnaires are verified.
- Separate the reinterview process from the field operation it is evaluating.
- Develop a management reporting process for quality assurance.



INVESTIGATIVE HIGHLIGHTS

FORMER CENSUS EMPLOYEE CONVICTED OF THEFT OF DEBIT CARDS

We previously reported the arrest of a former Census field representative in Santa Ana, California, on charges that she had cashed 16 debit cards given to her for use as incentives for survey participants. (See March 2002 issue, page 91.) On April 5, 2002, the defendant was convicted of grand theft and embezzlement in Orange County Superior Court, and was sentenced to 45 days in jail and 3 years' probation, and ordered to make restitution of \$1,180 to the government. (*DENVER FIELD OFFICE OF INVESTIGATIONS*)

⁷ U.S. Department of Commerce, Office of Inspector General, September 2000. *Reenumeration at Three Local Census Offices in Florida: Hialeah, Broward South, and Homestead*. Report No. ESD-13215.

MINORITY BUSINESS DEVELOPMENT AGENCY

The Minority Business Development Agency

was created to help minority-owned and operated businesses achieve effective and equal participation in the American free enterprise system, and overcome the social and economic disadvantages that have limited their participation in the past. MBDA provides management and technical assistance to minority firms upon request, primarily through a network of business development centers. It also promotes and coordinates the efforts of other federal agencies in assisting or providing market opportunities for minority businesses.

MBDA'S MINORITY BUSINESS OPPORTUNITY COMMITTEE PROGRAM

MBOC seeks to promote full inclusion of the minority business sector in the nation's economic infrastructure by providing a variety of programs to minority business owners interested in effectively marketing their products and services locally. MBOCs provide current business information; identify potential sales opportunities, financing resources, and joint venture partners; and give other appropriate support to position these enterprises for long-term growth.

DEFICIENCIES AND NONCOMPLIANCE FOUND IN CALIFORNIA MBOC OPERATIONS

A city in southern California has received continuous funding to operate an MBOC since January 1994, initially through noncompetitive joint project agreements and later through competitively awarded cooperative agreements. The city assigned responsibility for the MBOC award to the mayor's Office of Economic Development, with MBOC staff assuming responsibility for day-to-day administration of the agreement.

We performed a financial and compliance audit of three budget periods funded under the award—calendar years 1999, 2000, and 2001. Our purpose was to determine whether the recipient was performing in accordance with award objectives; claiming project costs that were reasonable, allowable, and allocable; and maintaining administrative requirements and controls that complied with award terms and conditions. Total estimated cost of the project for the 3 years was \$2,144,765, with the federal share not to exceed \$1.3 million.

Overall, we found that the city's performance was deficient in several respects and that it failed to comply with several uniform administrative requirements and federal cost principles. As a result of the noncompliance, we questioned costs of \$424,438 and recommended that MBDA reduce total allowable project costs by an additional \$408,430 in program-related income. Our specific findings are detailed below.

Performance deficiencies

The city's claims for a key performance measure—the dollar value of contracts and procurements generated for minority business enterprises (MBEs)—were not always accurate or supported. Included in the count were opportunities produced by and claimed for other programs administered by the MBOC with funding from other agencies—including Commerce's Economic Development Administration (see page 24) and the Department of Transportation (DOT). Claims for these opportunities resulted in multiple reports of the same contracts and procurements and a consequent overstatement of the MBOC's influence and accomplishments.

In addition, the MBOC served a broader clientele than was authorized under the award, and its organization and operations were not clearly established or documented.

Opportunities Produced by or Claimed for Other Funding Sources

Other Funding Source	Dollar Value of Procurements Claimed	
	Total	MBE
Calendar Year 1999		
DOT/EDA	\$ 49,724,194	\$ 4,872,043
DOT/EDA	249,715,762	110,743,217
DOT/EDA	115,301,272	115,301,272
DOT/EDA	42,518,194	40,267,949
DOT/EDA	722,840	17,600
DOT	47,011,598	3,143,838
Total for CY 1999	\$504,993,860	\$274,345,919
Calendar Year 2000		
DOT	\$ 113,814,388	\$ 12,116,262
DOT	36,277,372	2,848,410
DOT/EDA	132,130,868	41,180,356
DOT/EDA	166,845,170	54,763,227
HUD	1,884,073	245,351
Total for CY 2000	\$450,951,871	\$111,153,606
Calendar Year 2001		
DOT/EDA	\$ 20,065,137	\$ 1,944,910
DOT/EDA	391,134,061	132,092,858
Total for CY 2001	\$411,199,198	\$134,037,768

We recommended that the city be required to upgrade procedures for compiling statistics to (1) ensure the reported dollar value of contracts and procurements is complete, current, consistent, accurate, and verifiable; (2) reflect only contracts awarded to MBDA-defined minority business enterprises for the stated reporting period; and (3) claim actions that result solely from MBDA funding to the MBOC.

In addition we recommended that the city be instructed that efforts expended for beneficiaries other than those qualifying as MBDA-defined minority business enterprises are unallowable under the cooperative agreement and, if the MBOC continues to serve ineligible beneficiaries, it must establish a cost accounting system that identifies, segregates, and accounts for ineligible activities and excludes those costs from MBDA award reporting.

We also recommended that the city be directed to clearly establish and verify the organizational structure and the procedures of the award-funded entity and document ongoing operations.

Noncompliance

The city failed to comply with federal requirements for managing financial assistance awards and adequately supporting costs allowable for federal participation. Specifically, it did not implement key management controls for procurement, program-related income, and financial management systems. This failure led to a variety of problems: for example, consulting agreements were duplicative and not competitively procured; program income was not properly reported to MBDA and unused program income was not used to offset allowable costs; time and labor expenses were not adequately supported; and rates for calculating fringe benefits and indirect costs were not properly applied. These deficiencies and others we identified weakened the recipient’s control over both the project and award funds.

We recommended, for the years audited, that the Commerce grants officer disallow \$832,868 (\$424,438 in questioned costs plus \$408,430 in offsets to allowable costs) of the \$2,074,886 in project costs claimed; recover the federal share (\$499,746) of the disallowed amount; and notify the city that

1. it may not use MBDA funds to cover costs claimed and incurred under inappropriately procured consulting contracts;
2. it must comply with requirements for identifying, recording, reporting, protecting, and using program-related income in the approved budget period and through official recipient accounts and financial management and procurement systems; and
3. it must apply all unexpended program-related income at year-end against total allowable project costs.

In addition we urged the grants officer to confirm the city’s claims, made subsequent to our audit, that time and labor expenses are being properly documented; and ensure that the city correctly calculates fringe benefits and indirect costs charged to the award.

Interagency funding issues

The financial and compliance deficiencies we found in our audit of the MBDA cooperative agreement parallel those uncovered in a separate audit of EDA grants the city is using to fund a business outreach program, also operated by that city’s MBOC (see page 24). Therefore, we recommended that the Department’s grants officer coordinate with MBDA and EDA in overseeing the effective and timely resolution of issues common to both awards. *(SEATTLE REGIONAL OFFICE OF AUDITS: STL-14900-1)*



NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

The National Oceanic and Atmospheric Administration

studies climate and global change; ensures the protection of coastal oceans and the management of marine resources; provides weather services; and manages worldwide environmental data. NOAA does this through the following organizations:

National Weather Service reports the weather of the United States and provides weather forecasts and warnings to the general public.

National Ocean Service issues nautical charts; performs geodetic surveys; conducts research; and develops policies on ocean mining and energy.

National Marine Fisheries Service conducts a program of management, research, and services related to the protection and rational use of living marine resources.

National Environmental Satellite, Data, and Information Service observes the environment by operating a national satellite system.

Office of Oceanic and Atmospheric Research conducts research related to the oceans and inland waters, the lower and upper atmosphere, space environment, and the Earth.

Office of Marine and Aviation Operations operates NOAA's ships and aircraft and provides NOAA programs with trained technical and management personnel from the nation's seventh unified service.

TRAVEL CARD PROGRAM AT OAR'S ENVIRONMENTAL TECHNOLOGY LABORATORY IS GENERALLY SOUND, BUT COULD BENEFIT FROM TIGHTER INTERNAL CONTROLS

As part of our focus on government charge card operations at Commerce, we completed an assessment of the travel card program at the Environmental Technology Laboratory (ETL)—a component of NOAA's Office of Oceanic and Atmospheric Research (OAR).

The General Services Administration began the government travel card program to control travel payments and expenses. Regulations mandate that federal employees use the card when on official travel, unless they have been exempted from doing so. Employees are responsible for all costs charged. All uses other than for official travel are strictly forbidden. Those who misuse the card or fail to pay undisputed amounts are subject to disciplinary action, and can have the cards canceled and their wages garnished.

Our audit sought to determine whether ETL's internal controls over travel cards adequately ensured proper use and prompt payment by employees. We focused on charges incurred during FY 2001.

We found that with few exceptions, ETL employees used the travel card appropriately and paid their bills on time. However, certain internal controls were not strictly implemented, a situation we believe leaves open the possibility for problems. Specifically, we noted the following:

1. ETL did not have a list of all cardholders, so managers could not readily identify which employees had cards and ensure that the cards were issued only to those who truly needed them.
2. When cardholders left ETL employment, the laboratory did not always send copies of their destroyed cards to the travel card program coordinator—a required procedure that helps ensure departing employees no longer have access to their travel card accounts.
3. Three ETL employees used their travel card to pay for non-travel-related business expenses such as journal subscriptions, which should properly have been charged to purchase cards.
4. Three employees charged conference registration fees to their travel cards. These costs are expenses of the office and can be paid directly by the government agency.

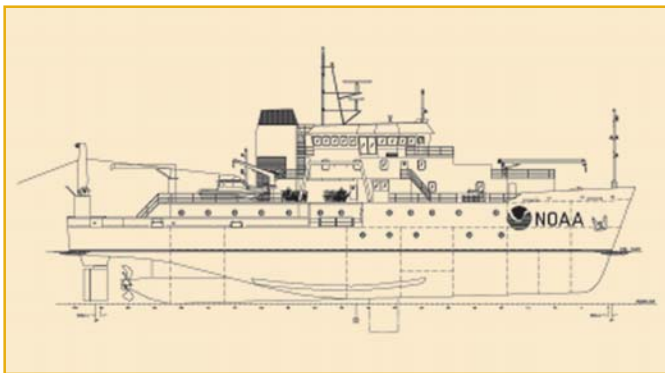
To strengthen ETL's monitoring of the travel card program, we recommended that ETL management develop and keep current a list of cardholders; take prompt action to close travel accounts of former employees by submitting destroyed cards and appropriate paperwork

to the NOAA travel card program coordinator and following up to ensure the accounts are closed; discontinue the practice of using travel cards to pay for business expenses not specifically related to travel; and send annual reminders to cardholders regarding what constitutes appropriate travel-related charges (e.g., transportation services, lodging). (*BUSINESS AND TRADE AUDITS DIVISION: BTD-14908*)

WEAK MANAGEMENT CONTROLS HAMPER NOAA'S EFFORT TO UPGRADE ITS FLEET OF RESEARCH VESSELS

NOAA's National Marine Fisheries Service (NMFS) relies heavily on at-sea research to fulfill its mission of protecting the nation's living marine resources, and uses a fleet of nine fisheries research vessels (FRVs) to conduct a variety of science-based ocean activities. Eight of these ships were constructed during the 1950s and 1960s, and all are fast approaching the end of their service lives.

NOAA is in the process of upgrading this fleet with up to four new state-of-the-art research vessels, to be built under its high-priority FRV-40 acquisition program. These ships will enable NMFS to stay at sea for as long as 40 days and to conduct a wider range of scientific studies.



NOAA reports that this state-of-the-art ship will be its first acoustically quiet fisheries research vessel capable of conducting a variety of scientific missions including fisheries stock assessments, physical and biological oceanography, marine mammal research, and atmospheric and sea surface research. It will provide the best available data to rebuild and sustain our fisheries and to meet the global challenge of maintaining sustainable ecosystems and protecting the integrity of long-term research analyses.

Source:
http://www.nmfs.noaa.gov/BudgetFactSheets/YOTO_FISHSHIPS.pdf

In September 1998 NOAA formed a project team consisting of representatives from several of its components to procure the vessels and manage the acquisition. Congress appropriated \$59.7 million in FYs 2000 and 2001 for design and construction of the first FRV and for management of the acquisition effort. NOAA planned to use another \$5.4 million in FY 2002 for managing acquisition of subsequent vessels. If all four ships are constructed, costs could exceed \$200 million.

In January 2001 NOAA awarded a contract to design and build the first vessel, but there have been problems since the outset. The contractor had difficulty meeting the bonding requirement, which delayed initiation of the work. Subsequently, the firm's parent company and its affiliates (including the contractor) filed for reorganization protection under the U.S. bankruptcy code. Although the company's future is uncertain, the firm has continued the contract work.

We conducted an audit of the FRV contract to (1) determine whether construction of the vessel was meeting the program's performance goals for cost and timeliness; (2) evaluate corrective action NOAA has taken or will take for any deviations from goals; and (3) assess the effectiveness of NOAA's management controls over the acquisition program. We identified a number of weaknesses in those controls, some of which rendered NOAA unable to provide the documentation we needed to achieve our first two objectives. We therefore recommended that NOAA take the following actions to improve management controls and thus ensure that the contract work proceeds efficiently for the first and all subsequent vessels:

- **Comply with federal requirements for contract files.** The FRV project team has not established an official contract file that contains all essential documents relating to the FRV acquisition, as required by the Federal Acquisition Regulation (FAR). Without this file, NOAA cannot effectively document procurement actions and decisions.
- **Enforce the contract's scheduling requirements.** The contractor has not provided NOAA with updated schedules, as required by both the contract and FAR, so neither party can systematically and objectively track the progress and timeliness of the contract work.
- **Strengthen procedure for tracking FRV program costs.** The reporting procedure established by the project team does not generate critical cost accounting and cost-goal information that the acquisition/program manager needs to monitor whether the FRV project is staying within cost goals. NOAA should amend this procedure for periodic financial reporting to include all essential information needed to direct the program.
- **Immediately implement a detailed award fee plan.** At the time of our audit, NOAA had yet to implement an effective award fee plan to encourage superior

performance by the contractor. The current plan lacks definition; clear, results-oriented evaluation criteria; examples of significant events that constitute superior performance; and detailed guidance for evaluators. Each day that passes without an acceptable plan in place compromises the contractor's ability to excel and increases the risk that goals for cost, performance, and product delivery will not be met.

- **Institute a clear, well-documented program management structure.** The current organizational structure of the project team does not clearly delineate and document specific authorities and responsibilities for individual team members, nor does it specify lines of communication and reporting relationships. This lack of specificity compromises the team's efforts to administer the contract effectively and increases the possibility of missed project milestones, friction among team members, and high turnover among project staff.

Two other weaknesses emerged during our audit that also require action. First, we found that NOAA did not conduct a preaward survey for the FRV contract. A preaward survey is an assessment of a potential contractor's ability to fulfill contract requirements. By failing to take this step, NOAA missed some key indicators of the contractor's uncertain financial status. NOAA should conduct preaward surveys for any future FRV contracts to be certain of choosing a financially sound contractor.



Columbia River Basin.

Second, we found that NOAA has no written contingency plan to ensure the uninterrupted flow of scientific data, should delivery of the research vessels be significantly delayed or the contract terminated. It must develop such a plan to ensure NMFS' ability to fulfill its stewardship role for the marine environment.

AGENCY RESPONSE

NOAA concurred with all but one of our recommendations—that a detailed award fee plan be developed and implemented immediately. While the agency agreed that such a plan was needed and has begun developing one, it believes implementation should be delayed until the contractor's bankruptcy status is resolved. We contend, however, that the plan is needed now because contract work continues despite the bankruptcy filing. (*SCIENCE AND TECHNOLOGY DIVISION: STD-14428*)

STRONGER MANAGEMENT RESEARCH PROCESSES AT NORTHWEST FISHERIES SCIENCE CENTER WOULD ENHANCE SALMON RECOVERY EFFORTS

The National Marine Fisheries Service (NMFS) is responsible for preventing the extinction and protecting the habitats of marine fish, mammals, sea turtles, and anadromous fish (salmon and other species that migrate between the ocean and inland waterways). In the Pacific Northwest, NMFS's endangered species activities are handled primarily by its Northwest Regional Office and Northwest Fisheries Science Center.

The regional office identifies and lists species that are endangered or threatened in its area of coverage, which encompasses much of the Columbia River Basin and large stretches of the Pacific Ocean. It creates management policies and plans to protect the listed species and their habitat, and works with groups whose proposed projects could harm the listed species to mitigate the harm. The science center, in turn, supports the region by assessing the status of all species and conducting scientific research to determine how best to protect and recover them and their habitats. The center has a large groundfish program and conducts research on a variety of other marine species, but much of its activities focus on Pacific salmon.

In 2000 the NMFS regional office issued a biological opinion on ways to mitigate the impacts of federally operated dams, powerhouses, and associated reservoirs on salmon migration up and

down the Columbia and Snake Rivers. Despite the center's years of salmon research, it discovered that it lacked basic scientific information—such as population estimates and the impact of various risk factors on population growth—needed to provide pertinent direction for actions affecting salmon. In response, it developed the Salmon Research Plan. Built on a framework of 10 broad questions (and numerous, specific subquestions), the plan sets an ambitious, interdisciplinary agenda for salmon recovery designed to ensure that center projects directly further recovery efforts.

We conducted a performance audit to assess management controls used to implement the plan, specifically focusing on (1) procedures for obtaining peer review, (2) strategies and processes for implementing the plan, and (3) methods for ensuring that ongoing work answers the 10 research questions. To determine appropriate controls for a science research program, we reviewed relevant guidance from OMB, the National Academy of Science and its National Research Council, the U.S. General Accounting Office, and other organizations.

We concluded that the Salmon Research Plan is an important step toward meeting the center's goal of strengthening its salmon research program. The plan establishes research priorities and supports NMFS's strategic goal of recovering and maintaining endangered species. In developing the plan, the center followed best practices for building solid research programs and incorporated elements that satisfy some of OMB's subsequently issued criteria for supporting the President's FY 2004 science agenda. The OMB criteria direct managers to create well-conceived plans that, for every program, (1) identify goals, priorities, and links to national and "customer" needs; (2) justify how funds will be allocated to ensure quality; and (3) implement appropriate outcome measures and milestones for tracking progress toward goals and assessing whether funding should be increased or redirected. The Salmon Research Plan already demonstrates progress toward meeting these criteria. With some additional work, it can more clearly reflect them.

Our other findings and recommendations are as follows:

Peer review. Despite the many positives of the research plan, its true value for improving the quality of the center's salmon-related work has not been rigorously evaluated via a documented peer review process. Although the center conducts peer review of some products, it does not have a documented peer review policy or a well-defined process for performing such reviews of its research plans. NMFS needs to issue guidance that clearly delineates the requirements for documented peer review processes. The science center should then document its existing process, add a step for obtaining formal comment on research

plans, and use this revised process to formally peer review the Salmon Research Plan.

Multiyear plans. A multiyear plan is a management control that takes broad objectives, such as those posed by the 10 questions in the Salmon Research Plan, and details a blueprint for measuring progress toward achieving them from one year to the next.

Multiyear plans (1) provide a framework for integrating research programs across functional and organizational boundaries; (2) establish a mechanism for evaluating ongoing research, identifying data gaps, and involving stakeholders; (3) allow transparency for programs by providing interim performance measures that link to longer term strategic goals; (4) enhance efforts to obtain needed resources; and (5) provide methods to better anticipate, evaluate, and complete research activities within realistic time frames.

At the time of our review, the center had developed multiyear plans for only 3 of the 10 research questions, and had given regional managers only limited involvement in decisions related to the Salmon Research Plan. We advised the science center to develop appropriate multiyear plans, work with regional staff to identify potential funding for projects in these plans, and subject the plans to appropriate peer review. We also noted that management at the center and the regional office need to establish a reliable method for involving the region and other stakeholders in developing the multiyear plans.

Processes for managing ongoing work. We found that the center lacked adequate controls for (1) documenting how ongoing research is answering the questions in the plan; (2) ensuring that its annual planning and project approval process documents the specific ways in which proposed work will support the plan; and (3) tracking actual time spent on projects—data needed to make informed decisions about costs and funding levels. The science center should assess and document the extent to which existing projects support finding answers to the salmon questions, clearly link the Salmon Research Plan to its annual planning and project approval process, and implement a system to track full program costs. In addition, we believe the center should make the research questions a standard component of its program review criteria. Program reviews are a form of peer review in which experts from within and outside an agency evaluate the relevance of research to agency goals. Including the 10 questions in the review criteria would further document a program's value in relation to the Salmon Research Plan.

NOAA agreed with our recommendations and added that all of its NMFS science centers could benefit from taking similar actions. (SCIENCE AND TECHNOLOGY AUDITS DIVISION: STD-14440)

FISCAL MISMANAGEMENT FOUND IN AUDIT OF NOAA COOPERATIVE AGREEMENT

A nonprofit fisheries research organization received a 3-year cooperative agreement from NOAA in April 1998. The \$3,207,915 award was to be used for research on protecting and enhancing salmon species in the Pacific Northwest. The agreement specified 31 tasks that the recipient was to complete.

Our audit, conducted in April 2002, sought to determine whether the organization had (1) accomplished the award objectives, (2) complied with federal regulations and award terms and conditions, and (3) claimed costs that were reasonable, allowable, and allocable.

Our review disclosed that the recipient failed to perform 8 of the 31 tasks required by the agreement and could not properly document the completion of work for the remaining 23. We also found that the organization had violated federal financial management regulations by inadequately managing the costs of the tasks. Specifically, it redirected the funds allocated for the 8 tasks it did not perform to other tasks; its financial reporting system did not compare actual expenditures against budgeted amounts for each task order, did not account for the 8 tasks that were not performed, and did not record the overexpenditures that occurred for 15 tasks; and the recipient’s expenses exceeded the project budget by \$11,674. The noncompliance with regulations and terms of the agreement and the inadequate administration of the award caused us to question \$428,695 in claimed costs.

Cost Category	Amount Questioned
Personnel	\$322,674
Fringe benefits	50,104
Indirect costs	55,917
Total	\$428,695

Because this was a cooperative agreement, NOAA personnel had substantial involvement in directing or redirecting the tasks to be performed, and apparently made significant modifications to the original work specified in the award. In light of this circumstance, we recommended that NOAA either amend the award to accurately reflect the actual tasks it directed the recipient to perform or disallow the total amount of questioned costs (\$428,695) and recover \$417,021 for the improper claims.

This research organization continues to perform work for NOAA under a different cooperative agreement. We therefore recom-

mended that for this second award, NOAA ensure the recipient performs all required tasks and carefully monitors incurred costs. (SEATTLE REGIONAL OFFICE: STL-14956)

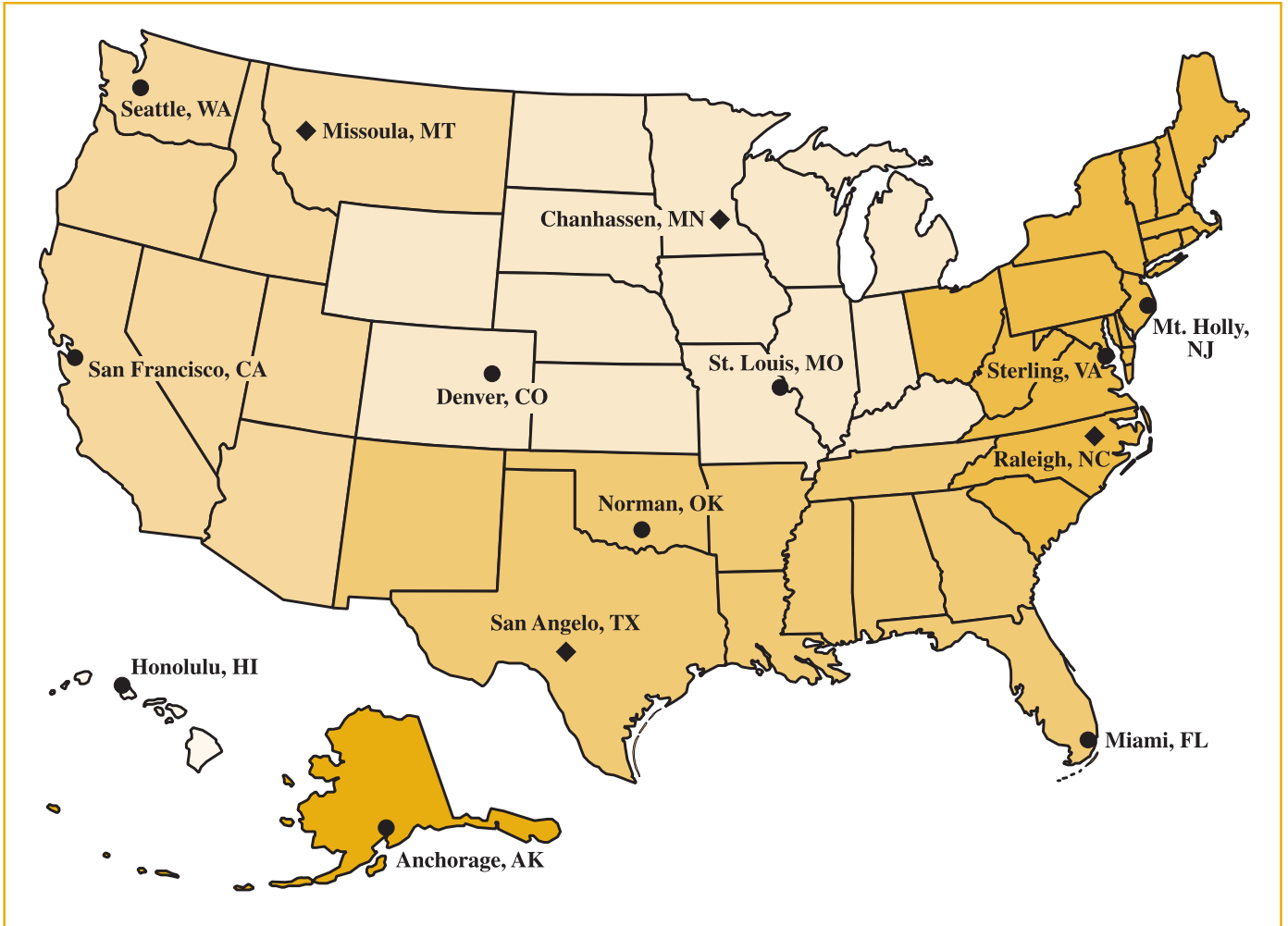


Artificial streambed located at NMFS field station.

ACCOMPLISHMENTS AND CROSSCUTTING ISSUES IDENTIFIED AT 14 WEATHER FORECAST OFFICES

The National Weather Service (NWS) operates 121 weather forecast offices (WFOs) nationwide, each of which provides continuous reports on weather conditions affecting its assigned county warning area. In FY 2000 OIG began inspecting these offices to determine how effectively they (1) deliver warnings, forecasts, and other information to their service users; (2) coordinate their activities with state and local emergency managers; and (3) supervise their network of volunteer observers and spotters. We also assessed each office’s management and internal controls; its compliance with Department, NOAA, and NWS policies and procedures; and the effectiveness of NWS’s regional oversight.

During previous reporting periods we completed comprehensive evaluations of four WFOs—Raleigh, North Carolina; San Angelo, Texas; Missoula, Montana; and Chanhassen, Minnesota—and found issues common to all. Specifically, we determined that the four generally provided effective weather services but needed to improve administration and management oversight. They also needed more attention from regional managers, who should conduct regular reviews of WFO management, program, technical, and administrative operations. (For more



Map shows WFOs where OIG performed complete inspections (◆) or limited inspections (●).

details about the Raleigh, Missoula, and San Angelo reviews, see the September 2001 issue, pages 43-49; for Chanhassen, see the March 2002 issue, page 57.)

During this semiannual period we conducted limited reviews of 10 additional offices—choosing WFOs from all six regions (see below)—to ascertain whether the strengths and weaknesses identi-

fied during our four comprehensive reviews existed elsewhere. We also followed up with the first 4 offices to document any improvements they had made since our initial inspections. At all 14 locations, we focused on the seven major areas of office operations defined by NWS: forecasting, outreach, the Skywarn and Cooperative Observer programs, staff training, information technology, office management/administration, and regional oversight.

Additional WFOs Reviewed

Eastern Region

Mt. Holly, New Jersey
Sterling, Virginia

Central Region

Denver/Boulder, Colorado
St. Louis, Missouri

Southern Region

Miami, Florida
Norman, Oklahoma

Western Region

San Francisco, California
Seattle, Washington

Alaska Region

Anchorage, Alaska

Pacific Region

Honolulu, Hawaii

SUMMARY OF FINDINGS

Overall, we found that the WFOs did a good job of providing reliable and timely forecasts and other weather products (such as warnings and advisories). We noted a number of operational strengths at the 10 offices and improvements at our original 4 inspection sites that we attribute to several circumstances: NWS's dissemination of our four comprehensive reports to all WFOs, its instruction to office managers to improve operations and procedures as necessary, and its formulation of a team of WFO meteorologists-in-charge to recommend techniques for improving operations. Among our specific findings are the following:

- NWS's forecast performance statistics for FY 2001 showed that 10 of the 14 offices had a good or satisfactory track record of accurately and expeditiously predicting weather events. The success rates for the remaining 4, however, were below regional averages. The regional offices and WFOs in question need to determine whether these statistics are an anomaly or a trend that needs correction.
- The offices conducted effective outreach activities to keep the community informed of weather events and to raise awareness of meteorology and weather safety.
- The WFOs we reviewed operate efficient and successful Skywarn and Cooperative Observer programs, with the exception of the Anchorage office, which faces formidable challenges because of the size and remoteness of its warning area and harsh winters.
- The offices generally provided good staff training. However, 7 offices did not have individual development plans in place for all employees (although they were slated to complete such plans by the end of FY 2002), and only 6 have active research agendas, even though NWS encourages the offices to conduct operational or applied research.
- Each of the 14 offices has security documentation in place for its information technology operations and on-site personnel to oversee IT security. They also implement IT controls and procedures, such as periodically revising passwords, updating software inventory, and testing office backup and contingency procedures.

At the same time, we found two administrative and management deficiencies that require attention:

- Most offices had weak internal controls over staff use of purchase cards, convenience checks, and vehicles, and maintained inadequate inventory records of accountable property. These deficiencies leave the WFOs vulnerable to waste and theft of government resources. We noted efforts to improve administrative operations at several

offices as a result of NWS's nationwide dissemination of our February 2000 report, which identified these problems at the Raleigh WFO.

- NWS regional offices did not provide adequate oversight of WFO management, program, technical, and administrative operations.

SUMMARY OF RECOMMENDATIONS

We made a number of recommendations to the assistant administrator for NWS to address the crosscutting issues we identified in our review of the 14 offices. Among these recommendations were the following: NWS regional directors should be instructed to (1) emphasize quality control of forecasts and forecast products to the WFOs and work with them to determine whether any of their state or local forecasts should be discontinued; (2) ensure that the Cooperative Observer Program remains fully staffed by trained employees, despite turnover; (3) ensure that the WFOs implement an office training plan, have individual development plans for all staff, and have appropriate training resources for the Weather Event Simulator and the Interactive Forecast Preparation System; (4) ask the offices to encourage their staff to conduct applied research and disseminate the research results via their Internet web pages; and (5) ensure that WFO managers and staff are properly trained to comply with regulations and guidelines for using purchase cards, convenience checks, and government vehicles, and for managing accountable property.

In addition we recommended that the various regional headquarters develop schedules to regularly visit and conduct comprehensive reviews of each WFO under their supervision, with particular focus on the office's programs, management, technical, and administrative functions, and IT security.

We also made a number of recommendations to address new or continuing problems identified at individual WFOs during this inspection. (*OFFICE OF INSPECTIONS AND PROGRAM EVALUATIONS: IPE-14577*)



INVESTIGATIVE HIGHLIGHTS

FORMER NOAA ADMINISTRATIVE OFFICER SENTENCED TO PRISON FOR EMBEZZLEMENT

In the September 2001 issue (pages 78-79), we reported the conviction of a former NOAA administrative officer on one felony

count of violating 18 U.S.C. §641, based on his embezzlement of more than \$33,000 from the government over a period of nearly 2 years. On May 14, 2002, the defendant was sentenced in U.S. district court for the Western District of Missouri to 5 months' imprisonment, 5 months' home detention, and 3 years' probation. Under the terms of his earlier plea agreement, the defendant is also required to make full restitution to the government. *(DENVER FIELD OFFICE OF INVESTIGATIONS)*

NEW HAMPSHIRE FISHERMAN INDICTED FOR GRANT FRAUD

On April 25, 2002, a four-count indictment was issued in the U.S. district court for the District of New Hampshire, charging a fisherman with false statements, fraud, and embezzlement in connection with a \$192,000 NOAA fishing industry grant awarded to a nonprofit organization to study the harvest and commercial development of green sea urchins. The indictment charged the defendant with claiming more than \$109,000 in salary and vessel time as project expenses, although he failed to perform the work set out in the grant agreement. In addition, he is charged with theft of approximately \$16,000 from the government by retaining the proceeds of sea urchin sales generated by the project. The false statement and wire fraud charges against the defendant each carry a maximum penalty of 5 years in prison, and the two theft counts could result in a sentence of up to 10 years' incarceration. Trial is scheduled for November 2002. *(WASHINGTON FIELD OFFICE OF INVESTIGATIONS)*

DEFENDANT ARRESTED IN FLORIDA ON WIRE FRAUD CHARGES

In the last issue (page 92), we reported the indictment of a former financial accounting technician at NOAA's Mountain

Administrative Support Center, who had manipulated the Commerce Administrative Management System to make about \$19,000 in payments to her personal credit card with government funds. On June 19, 2002, the defendant was arrested by an OIG agent and a federal marshal near Tampa, Florida, and released on \$25,000 bail after being arraigned on six counts of wire fraud. No date has been set for trial. *(DENVER FIELD OFFICE OF INVESTIGATIONS)*

FORMER NWS EMPLOYEE SENTENCED FOR MISUSE OF GOVERNMENT PURCHASE CARD

On April 5, 2002, a former employee of an NWS regional office in Alaska was sentenced in U.S. district court for the District of Alaska to 5 years' probation, based on her theft conviction for using a government purchase card to charge nearly \$7,500 in goods and services for her own use. (See March 2002 issue, page 91.) Under the terms of a plea agreement, the defendant is also required to make restitution of the full amount of the government's loss. *(DENVER FIELD OFFICE OF INVESTIGATIONS)*

GIFT ACCEPTANCE RESULTS IN NWS EMPLOYEE'S DEMOTION

In lieu of a proposed 14-day suspension, an NWS meteorologist agreed to a reassignment of duties and a voluntary reduction in grade for accepting gifts from an outside source in violation of the standards of ethical conduct for employees. An OIG investigation disclosed that the employee had received free tickets and parking passes from a minor league baseball team in appreciation for weather forecasts provided to the team by his office. *(DENVER FIELD OFFICE OF INVESTIGATIONS)*



NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

The mission of the National Telecommunications and Information Administration

is to (1) serve through the Secretary of Commerce as the principal executive branch advisor to the President on domestic and international communications and information policies, (2) ensure effective and efficient federal use of the electromagnetic spectrum, (3) develop with other federal agencies policies for international communications and standard-setting organizations, (4) serve as the federal telecommunications research and engineering center, and (5) administer grants under the Telecommunications and Information Infrastructure Assistance Program and the Public Telecommunications Facilities Program.

Advances in telecommunications continue to change the nation's economic and social fabric in ways that profoundly affect every American and the world at large: our marketplace, public services and protections, systems of education, and methods of information exchange are but a few of the fundamental aspects of society that rely on telecommunications technology.

NTIA's exclusive focus on telecommunications and information technology is unique among federal agencies, and puts it at the forefront of America's evolving communications infrastructure. In the new digital era, NTIA is using its expertise and resources to forge industry innovation and competition, as well as consumer empowerment; facilitate the availability of wireless services; and expedite the digital conversion of the public broadcast system.

NTIA's two telecommunications investment programs—the Technology Opportunities Program (TOP) and the Public Telecommunications Facilities Program (PTFP)—provide grants to state, local, and tribal governments, and nonprofit entities to help finance a range of telecommunications projects in underserved communities. TOP grants support model projects that demonstrate innovative uses of digital network technologies. PTFP grants support construction and replacement of public radio and television facilities, and expansion of broadcast signals. Since 1994 the two programs have awarded grants totaling approximately \$430 million.



INVESTIGATIVE HIGHLIGHTS

EMPLOYEE SUSPENDED FOR FALSE TRAVEL REIMBURSEMENT CLAIMS

Based in part on the findings of an OIG investigation, an NTIA employee received a 14-day suspension for filing multiple claims for reimbursement of local taxi fare charges that she had not actually incurred. (*SILVER SPRING FIELD OFFICE OF INVESTIGATIONS*)



TECHNOLOGY ADMINISTRATION

The Technology Administration serves the needs of technology-based industry, advocates federal actions and policies to speed the transfer of technology from the laboratory to the marketplace, and removes barriers for commercializing new technologies. It includes three major organizations:

Office of Technology Policy works to raise national awareness of the competitive challenge, promotes industry/government/ university partnerships, fosters quick commercialization of federal research results, promotes dedication to quality, increases industry's access to and participation in foreign research and development, and encourages the adoption of global standards.

National Institute of Standards and Technology promotes U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. NIST manages four programs: the Advanced Technology Program, the Manufacturing Extension Partnership program, a laboratory-based measurement and standards program, and the National Quality Program.

National Technical Information Service is a self-supporting agency that promotes the nation's economic growth and job creation by providing access to information that stimulates innovation and discovery. NTIS accomplishes this mission through two major programs: information collection and dissemination to the public, and information and production services to federal agencies.

INCREASING RELIANCE ON COMPUTING TECHNOLOGIES INCREASES VULNERABILITIES FOR NIST DATA

Automated teller machines, atomic clocks, mammograms, and semiconductors are among the innumerable products and services that rely in some way on the work of NIST. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. Most of NIST's work is done at two locations—Gaithersburg, Maryland, and Boulder, Colorado. The agency has a staff of more than 3,000 full-time scientists, engineers, technicians, and support personnel, plus 1,600 visiting researchers and 2,000 collaborators at affiliated centers around the country and overseas.

An ever-increasing amount of NIST's work depends on computer models, computer data, and other electronic information. With NIST's increasing reliance on computing technologies, including the use of the Internet and its related information dissemination techniques, the potential for loss, compromise, and misuse of NIST data and facilities has grown tremendously.

ADDITIONAL IMPROVEMENTS WOULD STRENGTHEN NIST'S INFORMATION SECURITY PROGRAM

As part of our review of Department-wide information security measures (see page 53), we evaluated NIST's security policies and procedures to determine their compliance with the Government Information Security Reform Act using NIST's *Security Self-Assessment Guide for Information Technology Systems*.⁸ We found that NIST is taking steps to improve information security; for example, it has increased its computer security staff, developed issue-specific policies, procedures, and guidance for handling a number of security concerns; posted to its intranet a system security plan template, guidance, and list of frequently asked questions to aid in security plan development; established a security awareness and training program; and implemented a computer security incident reporting and handling process. However, the

⁸ NIST, November 2001. *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication (SP) 800-26. Gaithersburg, MD: National Institute of Standards and Technology.

bureau has yet to meet a number of key GISRA and other federal requirements, and we made recommendations to resolve these deficiencies.

NIST's Information Security Policy and Procedures Need to Be Strengthened

The policy does not address critical roles and responsibilities and essential management control elements, such as risk management, review of security controls, and certification and accreditation.⁹ It assigns responsibility for system accreditation to the CIO, but not to the senior official whose mission the system supports.

We recommended that the director of NIST take the necessary steps to ensure the development and implementation of a comprehensive policy by instructing NIST managers to explicitly identify and document all information security roles and responsibilities, including those of the director and CIO; by extending accreditation authority to all senior officials whose mission could be adversely affected by information security weaknesses; and reviewing and revising, as appropriate, NIST's Recommended Computer Security Procedures for incorporation into the security program policy.

Deadlines for Risk Assessments, Security Plans, and Accreditations Are Unrealistic

At the time of our evaluation, none of NIST's 109 operational systems had a documented risk assessment or an approved security plan. Additionally, all but 2 systems lacked accreditation. The bureau had established a schedule for completing risk assessments, security plans, and accreditations, but we believe its time frame was too ambitious to permit sufficient analysis, documentation, and review.

NIST indicated that it had extended its deadline for accreditation by 30 days. However, given the complexity and importance of the activities required to accomplish accreditation, including testing of security controls to ensure that they perform as intended, we remain concerned that even with the schedule extension, there is not enough time to adequately complete all of the requisite activities and documentation. We believe that the accreditations should be considered provisional until there is confirmation that each system has all needed security controls and that these controls have been tested to ensure they perform as intended.

⁹ Certification is the formal testing of the security safeguards implemented in a computer system to determine whether they meet applicable requirements and specifications. Accreditation is the formal authorization by management for system operation, including an explicit acceptance of risk.

NIST's Inventory of Sensitive IT Systems Was Incomplete

We identified three operational systems from the Advanced Technology Program that were not included in the inventory, which suggests that systems in other NIST components may also be omitted. NIST publication SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, contains guidance for identifying systems subject to security controls. We recommended that the bureau make this information readily available to all of its components and see that it is properly followed. NIST noted that additional guidance was provided on system boundaries to system owners, who used it to reassess the system inventory.

User Accounts for Off-Site Researchers Are Not Always Promptly Closed When Access Is No Longer Required

NIST needs to tighten this control: bureau managers should verify that systems administrators and information security officers are immediately notified when external researchers no longer need access to NIST's computing resources. NIST stated that in FY 2001, it began developing a system for tracking guest researchers who have a NIST badge and that the system will be expanded to track all guest researchers and external collaborators.

Risk Designations for Some Positions Are Inconsistent with Their Levels of Responsibility and Trust

Designations of risk reflect the potential damage an individual in a position of public trust could cause to the efficiency and integrity of government programs. We found that some positions in the Advanced Technology Program and the Mechanical Engineering and Physics laboratories—such as systems administrators and information security officers—had low risk designations, even though the work of such staff directly affects government operations. As a result, employees in these positions had not received appropriate background checks. NIST responded that its managers have been instructed to work with the Department's Office of Human Resources and Office of Security to verify that all current positions are properly designated according to risk and appropriate background investigations conducted for staff who have information system or security responsibilities.

NIST Does Not Have an IT Capital Asset Planning Process

The 1996 Clinger-Cohen Act requires agencies to establish a capital planning and investment control process for all IT capital

assets to help ensure that appropriate projects are funded and well managed and to integrate IT planning, budgeting, acquisition, and management. GISRA and OMB require agencies to identify and budget for security measures and resources needed to protect their IT investments throughout the investment's life cycle. Despite these and other federal directives, NIST has yet to implement an agencywide IT capital planning and control process, and thus cannot ensure that IT projects are appropriately selected, planned, and managed; that information security is a factor in each system's design and a management consideration throughout its life cycle; or that information security cost estimates are valid. The bureau should set and meet a deadline for finalizing and implementing an IT capital planning and investment control process that integrates information security with the budget process. According to NIST, a capital investment planning process was begun in FY 2002 and will be fully implemented in FY 2003.

NIST Needs a Permanent Chief Information Officer

To support GISRA requirements for executive oversight of information security improvements, in June 2001 the Secretary of Commerce directed all operating units to appoint a CIO who would report to the unit's head or principal deputy, as well as to the Department's CIO. The Secretary further directed secretarial officers and heads of operating units to give information security high priority and sufficient resources and to work closely with their CIOs to implement effective security measures.

At the time of our review, NIST had not appointed a CIO. Instead, its CIO office resided in its Information Technology Laboratory (ITL) and reported to ITL's acting director, who also served as the acting CIO. NIST needs to define and implement a new CIO organizational structure, appoint a CIO as soon as possible, and ensure that this official has responsibility for and authority to develop and maintain an agencywide information security program. NIST should also take other appropriate actions to ensure that information security receives high priority in accordance with the Secretary's direction and that senior management officials at the bureau understand and implement their information security responsibilities.

AGENCY ACTIONS ON OUR RECOMMENDATIONS

NIST has accepted and is implementing our recommendations. Since the conclusion of our fieldwork, the director of NIST issued several memorandums acknowledging his responsibility for the security of NIST's data and IT systems and directing upper management to give information security high priority. He also directed upper management to ensure the agency's policies,

procedures, and operational environment are exemplary. NIST's CIO will co-accredit all systems after a review by the information security officer. Finally, a proposal for a new CIO organization was submitted to the Department for approval. (*OFFICE OF SYSTEMS EVALUATION: OSE-15078*)

ADVANCED TECHNOLOGY PROGRAM

Since 1990 the Advanced Technology Program (ATP) has invested nearly \$1.9 billion in private sector research and development to accelerate the time-to-market for innovative technologies that promise significant benefits to the nation as a whole. ATP develops partnerships with individual firms (single applicants) or consortiums of businesses (joint ventures) as well as with universities and nonprofit organizations, entering into cooperative agreements to share the cost of high-risk research and development.

From 1990 through June 2002, NIST awarded 414 ATP agreements to single applicants and 188 agreements to joint ventures. Small businesses constituted 75 percent of the single applicants and were the lead firm in 36 percent of the joint ventures.

Joint ventures have accounted for approximately 60 percent of total ATP funding and averaged \$6 million per agreement, while awards to single applicants averaged \$1.8 million. Private industry has matched ATP's investment with \$1.8 billion over the program's 12-year history. ATP's cost-sharing requirements are strict: joint ventures must pay at least half of the project costs. Large Fortune 500 firms participating as single applicants must pay 60 percent. Small and midsize firms may be reimbursed for up to 100 percent of direct costs, but must pay all indirect costs.

During this semiannual period we audited costs claimed under five ATP awards—three joint ventures and two individual awards.

AUDIT OF PENNSYLVANIA JOINT VENTURE ADMINISTRATOR QUESTIONS \$3.3 MILLION IN CLAIMED COSTS

In September 1995 NIST awarded \$21.3 million in ATP funds to a nonprofit corporation located in western Pennsylvania as the designated joint venture administrator of a consortium of businesses developing a national health care "knowledge bank"—a searchable multimedia database of expert medical information that doctors can browse and retrieve. Estimated costs for the 5-year project were \$51.3 million, of which joint venture members

were required to contribute \$30 million. ATP funding concluded in September 2000. Over the course of the 5 years, the administrator claimed \$8.6 million in direct costs and \$3.1 million in indirect costs.

We sought to determine whether the administrator’s claims for reimbursement of direct project costs were accurate and whether it had complied with applicable legal and administrative requirements. Our audit disclosed that the administrator claimed \$3,255,490 in unsupported or otherwise unallowable costs in the following categories:

Questioned Costs	Amount
Salaries and fringe benefits	\$ 354,475
Equipment	669,989
Consulting	1,130,700
Network contracts	1,100,326
Total	\$3,255,490

We recommended that NIST disallow the full amount questioned and recover \$1,466,754 in excess federal disbursements. A separate audit of the project’s indirect costs is currently under way. (ATLANTA REGIONAL OFFICE OF AUDITS: ATL-13993)

OIG RECOMMENDS DISALLOWANCE OF COSTS AND RECOVERY OF FUNDS FROM NEW JERSEY JOINT VENTURE

In September 1998 NIST awarded an ATP cooperative agreement to partially fund a joint venture for development of propane-fueled power systems to support telecommunications applications. The 2-year project had total estimated costs of \$6,376,772, with the federal share capped at \$3,159,324, or 49.54 percent of allowable costs.

For the 2-year award period ending December 31, 2000, the two participants in the joint venture claimed total costs of \$5,915,528. NIST reimbursed \$2,929,018, which left \$230,306 in undisbursed award funds. The administrator subsequently submitted additional claims that extended beyond the approved award period, which NIST has not reimbursed.

We audited the total claimed costs by the two businesses in the joint venture. We confirmed that the accounting systems used to administer the award were generally adequate and that the

joint venture members were materially in compliance with award terms and conditions. However, we questioned \$367,014 of the total costs for which the two businesses received reimbursement—\$350,142 in indirect costs that exceed the budgeted amount and negotiated rate, and \$16,872 in labor and consulting costs incorrectly charged to the NIST project. We also determined that claims submitted for costs incurred beyond the approved project period were ineligible for NIST reimbursement.

We recommended that NIST disallow the questioned costs, recover disbursed federal funds of \$180,284, immediately close out the award, and deobligate the remaining award funds so that they can be put to better use. (DENVER REGIONAL OFFICE OF AUDITS: DEN-14978)

MINOR INFRACTIONS FOUND DURING AUDIT OF TEXAS JOINT VENTURE PARTICIPANTS

A joint venture is conducting a \$5.8 million broadband communications project under a 30-month ATP cooperative agreement. Federal funding for the project is limited to \$2,395,768, and the award period is November 2000 through April 2003.

We conducted an interim audit of \$1,957,530 in costs claimed by all the participants in the joint venture administrator from the project’s inception through March 2002. We also assessed the administrator’s accounting and financial systems and compliance with ATP terms and conditions.

We found that the administrator billed NIST twice for sales tax (\$15,722) on an equipment purchase and improperly charged \$7,075 for related general and administrative costs. We questioned this total amount (\$22,797). The administrator agreed with our finding and deducted the amount from its March 2002 request for NIST reimbursement. We found no other deficiencies with the administrator’s accounting system and no instances of noncompliance with applicable laws and regulations. (DENVER REGIONAL OFFICE OF AUDITS: DEN-14517)

CONFLICT OF INTEREST RESULTS IN QUESTIONING OF COSTS CLAIMED BY CALIFORNIA RECIPIENT

In September 1998 NIST awarded an ATP cooperative agreement to a single applicant for a 3-year research project that had total estimated costs of \$2,279,524. Federal funding for the project was capped at \$2 million.

Our audit sought to (1) determine whether the recipient's accounting and financial management systems complied with federal regulations and NIST/ATP requirements, (2) verify final incurred costs, and (3) identify any instances of noncompliance with award terms or conditions.

We noted a conflict of interest in the recipient's awarding of two subcontracts and one consultant agreement: both the subcontractor and the consultant were members of the recipient's board of directors and thus had the ability to influence their selection as service providers and the administration of the resulting contracts and agreements. Additional questioned costs totaling \$9,652 were comprised of (1) \$6,962 in postaward costs, (2) \$2,286 in commercialization costs, and (3) \$404 in fines. As a result, we questioned \$540,913 in subcontractor and consultant costs. *(DENVER REGIONAL OFFICE OF AUDITS: DEN-14886)*

NO COST OR COMPLIANCE ISSUES NOTED IN INTERIM AUDIT OF MASSACHUSETTS RECIPIENT

We performed an accounting system survey and interim financial and compliance audit of an ATP cooperative agreement award to a Massachusetts firm in March 2001. Total estimated costs for the 2-year project were \$1,992,245, with federal funding during the first year limited to \$1,128,000.

We reviewed project costs claimed during the first 9 months of the award—\$1,269,000, for which the recipient received reimbursement of \$846,000. Our audit found that the claimed costs were accurate and appropriately reimbursed, the firm's accounting system was generally adequate for the purposes of the award, and the company was adhering to award terms and conditions in all material respects. *(DENVER REGIONAL OFFICE OF AUDITS: DEN-14989)*

MANUFACTURING EXTENSION PARTNERSHIP PROGRAM

Manufacturing has long been a staple of the U.S. economy. More than 360,000 manufacturers employ some 18 million people and contribute a combined total of \$1.5 trillion to our annual gross domestic product. Two-thirds of the manufacturing workforce is employed by small and midsize firms.

To remain competitive, manufacturers must be able to stay abreast of ever-changing technologies and meet new global chal-

lenges. But the ability of small and midsize firms to integrate new technologies and related management practices, and thus enhance their performance and productivity, is often hindered by a lack of financial and technical resources.

The Manufacturing Extension Partnership Program (MEP) attempts to help smaller companies overcome these barriers by entering into cooperative agreements with industry experts to provide needed business and technical expertise. During this semiannual period, we audited one MEP cooperative agreement.

AUDIT DISCLOSES \$2.4 MILLION IN QUESTIONED COSTS AND MORE THAN \$600,000 IN UNREPORTED PROGRAM INCOME

In September 1996 NIST awarded an MEP cooperative agreement to a Minnesota firm for a business assistance project with a total estimated cost of \$33,037,125. Federal funding was not to exceed \$11,012,375, or 33.3 percent of allowable costs. The project was scheduled to run through June 2002.

We conducted an interim financial and compliance audit of costs claimed during the 2-year period from July 1999 through June 2001 to determine whether the recipient's accounting and financial management system complied with federal and MEP requirements and whether claimed costs were supported and allowable. As a result of our audit we questioned \$2,440,890 in administrative costs that the recipient had arbitrarily charged as direct costs, rather than indirect costs under an approved cost allocation plan, as required by the award and applicable cost principles. We also found that the recipient's accounting system did not accurately allocate labor and related costs among NIST and non-NIST functions; and the firm failed to report \$652,334 in program income. The \$2,440,890 in unsupported costs and the \$652,334 in unreported program income resulted in excess program income of \$3,093,224.

We recommended that NIST disallow the \$2,440,890 in unsupported costs and recover \$813,631 in excess federal disbursements. We further recommended that the firm be required to develop plans and procedures to correct its accounting and cost allocation deficiencies. Finally we recommended that the firm account for the \$3,093,224 in excess program income, which could be revised downward should unsupported costs be resolved. *(DENVER REGIONAL OFFICE OF AUDITS: DEN-14879)*



INVESTIGATIVE HIGHLIGHTS

NIST TO RECEIVE PAYMENT FROM ATP RECIPIENT TO SETTLE FALSE CLAIMS ACT ALLEGATIONS

A Utah chemical company that received nearly \$4 million in Advanced Technology Program funds has agreed to pay NIST between \$700,000 and \$1.2 million over the next 5 years to settle allegations that the company mischarged the government under two research awards. The settlement resolved a

qui tam (whistleblower) suit initiated by five former employees of the company, who alleged that the ATP awards had been charged for labor and other costs actually incurred to perform work for the company's commercial customers. The United States intervened in the action in May 1999, following an investigation of the charges by OIG with the assistance of a NIST chemist. The final amount of the settlement—the first False Claims Act settlement involving an ATP award—will be determined by the level of the company's gross income over the next 5 years; a share of the proceeds will be paid to the original plaintiffs under the act's whistleblower provisions. As part of the settlement, the company has also agreed not to participate in any nonprocurement program at Commerce for a 5-year period. (WASHINGTON FIELD OFFICE OF INVESTIGATIONS)



UNITED STATES PATENT AND TRADEMARK OFFICE

The United States Patent and Trademark Office

administers the nation's patent and trademark laws. Patents are granted, and trademarks registered, under a system intended to provide incentives to invent, to invest in research, to commercialize new technology, and to draw attention to inventions that would otherwise go unnoticed. USPTO also collects, assembles, publishes, and disseminates technological information disclosed in patents.

INDEPENDENT OIG EVALUATION OF USPTO'S INFORMATION SECURITY PROGRAM REVEALS WEAKNESSES BUT HIGH-LEVEL COMMITMENT TO IMPROVE

As a performance-based organization, USPTO has greater flexibility and independence in managing its operations and thus has undertaken actions separate from the Department to manage information security. Therefore, this year we conducted a separate GISRA evaluation of USPTO's information security program in addition to our review of the Department's (see page 53).

We sought to determine whether the bureau's program and practices comply with the act, which requires that agencies have effective security measures for the information resources that support their operations. We based our evaluation on the findings of the information security-related reviews of USPTO we conducted during the fiscal year.

Until recently, information security had not received adequate attention at USPTO. As a result, significant weaknesses exist in planning, budgeting, implementing, reviewing, and overseeing this area. We found that the bureau is making a determined effort to improve its information security program and its top leadership is committed to this goal. USPTO has developed a corrective action plan that provides a solid foundation for improvement. However, much remains to be done.

EVALUATION RESULTS

1. GISRA requires that significant deficiencies in security policy, procedures, or practices be reported as a material weakness. OMB instructs agencies to identify security weaknesses if there is no assignment of security responsibility, no security plan, or no accreditation. USPTO lacks up-to-date security plans and current accreditations for its operational systems—deficiencies we believe constitute a reportable material weakness. We recommended that USPTO report information security as a material weakness until all mission-critical systems are accredited. In its own GISRA report, USPTO stated that it had declared information security a material weakness in FY 2002 because none of its systems has been certified or accredited.
2. USPTO's incident response procedures are not consistent with requirements in OMB Circular A-130 and GISRA, in that they do not require the bureau to notify or consult OIG and external security offices and authorities about a significant security incident. USPTO is revising these procedures to stipulate that incidents be reported to the Department, which will then relay the information to the appropriate entities.
3. Program officials have not given sufficient attention to assessing the risks to the information assets that support their operations, determining the level of security required to protect them, and periodically testing and evaluating information security controls and techniques. We found that 82 percent of USPTO's operational systems lacked documented risk assessments; 30 percent had outdated security plans; and none had been accredited.
4. GISRA requires agency CIOs to administer the information security program agencywide, a process that entails developing the program, ensuring it is effectively implemented and maintained, and training and overseeing personnel who have significant responsibilities for information security. USPTO needs improvements in all of these areas. Specifically, at the time

of our evaluation, existing policies and procedures were often not implemented, security impacts of system upgrades were not always considered, system security documentation was inaccurate, information security training inadequate, and information security requirements were neither identified in capital asset plans nor linked to security cost estimates.

5. USPTO needs to include information security provisions in its IT service contracts, in light of the findings of our review of 40 such contracts throughout the Department (see page 51). Across the board, we found that provisions to safeguard sensitive but unclassified systems and information in these contracts (some of which had been awarded by USPTO) were either insufficient or nonexistent—a problem likely affecting the majority of IT service contracts throughout the Department.
6. At the time of our evaluation, meeting some important deadlines in USPTO's corrective action plan appeared problematic, including those for developing the administrative order on security policies, completing a certification and accreditation pilot, developing system-level procedures, and preparing a disaster recovery plan.

In addition to the actions described above, USPTO intends to have updated security plans in place by the end of FY 2002. It has funded development of a certification and accreditation process, with a goal of accrediting all high-risk systems by the end of FY 2003 and all remaining systems by the end of FY 2004. The process will include updates of security plans every 3 years.

USPTO is also restructuring the Office of Information System Security to increase its effectiveness; and the chief information officer is preparing an administrative order describing USPTO's information security policies and clarifying staff roles and responsibilities. In addition, all USPTO employees and contractors completed security awareness training as of June 30, 2002, and a working group is developing a plan for providing security training specific to the individual responsibilities of all staff members. USPTO has also developed an information security budget that allocates funding for needed improvements. (OFFICE OF SYSTEMS EVALUATION: OSE-15250)

USPTO IS ACTING TO RESOLVE SECURITY WEAKNESSES IN HIGH-PRIORITY PATENT APPLICATION CAPTURE AND REVIEW AUTOMATED INFORMATION SYSTEM

As part of our GISRA work, we evaluated USPTO's Patent Application Capture and Review Automated Information System, or PACR. This system captures, stores, maintains, retrieves, and prints digital images of U.S. patent applications and is thus critical to USPTO's daily operations. We used NIST's *Security Self-Assessment Guide for Information Technology* to assess implementation of a sample of PACR's management and operational controls for information security (see table below). We originally intended to assess technical controls as well, but opted not to because USPTO was unable to provide consistent information in this area and because the bureau will evaluate those controls as part of a pilot project it is conducting on certification and accreditation in response to our agencywide evaluation (see March 2002 issue, page 74). USPTO is implementing other recommendations from that evaluation, which should address many of the problems we identified in our PACR review.

MANAGEMENT CONTROLS

We noted weaknesses in all the management controls we assessed. However, weaknesses in the first four controls are being addressed as part of the pilot project.

1. **Risk management.** No risk assessment had been performed for PACR; therefore, we could not determine whether security measures were adequate to deal with existing threats and vulnerabilities.
2. **System security plan.** USPTO had developed security plans for PACR but could not document their official approval. Hence, PACR lacks a critical component needed for accreditation—an approved security plan.
3. **Review of security controls.** OMB requires that agencies perform a formal management review of security controls, which should include an independent assessment, at least every 3 years and whenever a significant system modification occurs. At the time of our evaluation, PACR controls had not been tested.
4. **Authorize processing.** OMB also requires that management officials formally authorize (accredit) the use of a system before it becomes operational, and reauthorize it whenever a significant change occurs or at least every 3

years. PACR has been upgraded several times since its implementation, but none of the versions have been accredited.

- Life cycle.** At the time of our review, USPTO was upgrading operations by switching to a more capable local area network, which required changes to PACR network components and related software. However, these changes were not well planned, nor did they adequately consider network security implications: just prior to the initial transition step for PACR, USPTO could not identify the necessary changes to software and firewall rules. The information systems security officer had not been notified of the impending firewall changes, even though, at the time, he was the acting director of the Office of Information Security, which is responsible for directing and reviewing such proposed modifications.

In addition, the PACR system documentation we reviewed did not reflect the current system and four network topology diagrams we examined had the same issuing date but each was different from the others and none accurately described the then-current or planned topology. Although they were describing the same system, the High-level Architecture document and the Operational Support Plan contained different information concerning the network topology, equipment lists, and points of contact. USPTO needs to improve its process for keeping documentation current and for tracking its status.

OPERATIONAL CONTROLS

The physical security measures in place during our review provided appropriate protection for equipment that PACR relies on to support USPTO operations. Servers that store images of patent applications, as well as the firewall that prevents unauthorized access to them, are located in a secure data center that has effective electronic entry controls and round-the-clock security personnel. Scanning servers that create the images are located in a separate secure facility, but USPTO plans to relocate them with the storage servers. We noted that in their current location, access is controlled by a cipher lock, the combination to which is not changed when employees and contractors who have access conclude their work with USPTO. We recommended that USPTO implement an agencywide policy for changing cipher combinations periodically as well as whenever an employee or contractor no longer requires access.

We found problems in the other two operational controls we assessed. Specifically, USPTO does not have a contingency plan to compensate for the loss of PACR operations in the event the system becomes nonfunctional, despite OMB requirements for such plans; and PACR system administrators have not received specialized security training tailored to their information security responsibilities.

SCOPE OF OIG REVIEW OF SECURITY CONTROLS FOR PATENT APPLICATION CAPTURE AND REVIEW SYSTEM

Control Category	Control	Assessed
Management	Risk Management	X
	Review of Security Controls	X
	Life Cycle	X
	Authorize Processing	X
	System Security Plan	X
Operational	Personnel Security	
	Physical Security	X
	Production, Input/ Output Controls	
	Contingency Planning	X
	Hardware and Systems Software Maintenance	
	Data Integrity	
	Documentation	
Technical	Security Awareness, Training, and Education	X
	Incident Response Capability	
	Identification and Authentication	
	Logical Access Controls	
	Audit Trails	

AGENCY RESPONSE

USPTO agreed with all of our recommendations and has begun taking action to address them. (*OFFICE OF SYSTEMS EVALUATION: OSE-14926*)



INVESTIGATIVE HIGHLIGHTS

FALSIFIED TIME AND ATTENDANCE RECORDS RESULT IN THEFT CHARGES

On September 23, 2002, a criminal complaint was filed in U.S. district court for the Eastern District of Virginia charging a former USPTO employee with nine counts of theft of government property. The charges were based on an OIG investigation, which disclosed that in her role as office timekeeper, she had inflated her reported hours of work over a 7-month period to obtain approximately \$7,000 in salary payments to which she was not entitled. The defendant is scheduled to appear for arraignment at the end of October. *(SILVER SPRING FIELD OFFICE OF INVESTIGATIONS)*

SENIOR USPTO OFFICIAL COUNSELED FOR APPEARANCE OF CONFLICT

A senior USPTO official was counseled for engaging in actions that created the appearance of a conflict of interest after an OIG investigation disclosed his participation in discussions and other activities involving an outside organization that was negotiating an employment arrangement with his wife. In an effort to eliminate any real or apparent conflicts in the future, the official was also assigned to head a new unit that—unlike his previous office—would not have direct responsibility for matters relating to his wife's employer. *(SILVER SPRING FIELD OFFICE OF INVESTIGATIONS)*



DEPARTMENT-WIDE MANAGEMENT

The United States Department of Commerce promotes job creation and improved living standards for all Americans by creating infrastructure that fosters economic growth, technological competitiveness, and sustainable growth.

The Department has three strategic goals:

Goal 1: Provide the information and the framework to enable the economy to operate efficiently and equitably.

Goal 2: Provide the infrastructure for innovation to enhance American competitiveness.

Goal 3: Observe and manage the Earth's environment to promote sustainable growth.

The Department has also established a Management Integration Goal that is equally important to all bureaus: **Strengthen management at all levels.**

STRONGER INTERNAL CONTROLS AND MANAGEMENT OVERSIGHT NEEDED IN THE OFFICE OF ADMINISTRATIVE SERVICES

The Office of Administrative Services (OAS), a component of the Office of the Secretary, provides administrative support to Commerce headquarters and various units, ranging from mail handling, printing, and library services, to property and vehicle management. In addition, OAS provides Department-wide policy and oversight in such areas as construction, energy conservation, and environmental management.

At the request of the Department's Chief Financial Officer and Assistant Secretary for Administration (CFO/ASA), we conducted an inspection of internal operations at OAS, specifically focusing on practices involving purchase card and cell phone use, cash awards, and overtime.

Overall, we found problems in each of the areas we evaluated, some of which were systemic, others that were limited to specific situations, and most of which were due to poor management practices and inadequate internal controls. We detailed a series of recommendations to resolve these problems in a report to the CFO/ASA, who responded with appropriate corrective action. Our key findings and recommendations, as well as departmental steps taken to address the deficiencies, are summarized below.

- **Purchase card use did not always adhere to policy.** OAS participates in the federal purchase card program, which is designed to streamline the process for making small purchases and reduce associated administrative costs and paperwork. Our examination of records for purchases made by 26 cardholders between March 2001 and March 2002 revealed that these employees did not always keep documentation to support purchases and did not use required sources of supply. For 8 percent of the purchases we reviewed, employees did not obtain the necessary approval.

We recommended that cardholders be required to keep a log of all purchase card transactions and retain all original documentation; that approving officials review the log and statement of account, reconcile and approve all purchases monthly, and ensure that cardholders secure services and supplies from mandatory sources unless they have written authorization to purchase from commercial sources. The Department agreed with our recommendations and has implemented procedures to ensure that OAS purchase card usage adheres to applicable policy.

- **Awards program was not well managed.** OAS employees received approximately \$508,476 in departmental awards during fiscal years 1999 through 2001. However, we found a disorganized awards process that was poorly supervised and had weak internal controls. As a result, Commerce guidelines were violated. Because we were concerned that the deficiencies might be symptomatic of a Department-wide problem, we issued a special memorandum to the CFO/ASA prior to completion of our review, to alert him to our findings and prompt him to take action without delay. (See box on next page for a full discussion of the problems we identified, our recommendations, and the Department's response.)

- **Cell phones were used for personal calls.** Some cell phone records appeared to contain calls that did not pertain to official government business, and monthly bills were sometimes exorbitant—frequently ranging from \$400 to \$800, and in two instances topping \$1,000. We recommended that OAS seek full reimbursement for personal calls from any employees who have yet to make such payment; develop written policies that clearly state appropriate and allowable use of government-issued cell phones; provide cell phones only to staff who absolutely need them to perform their jobs, and tailor their calling plan to expected monthly usage; and instruct managers to monitor cell phone bills for evidence of abuse and to take appropriate action.

The Department concurred with our recommendations and has established procedures to ensure that cell phones are used for official government business only and operate on the most economical service plan. In addition, OAS managers are reviewing cellular phone bills to determine the total amount that employees owe for personal calls.

- **Time and attendance controls and documentation were lacking.** We reviewed time and attendance records for three employees to verify overtime charges of 1,152 hours during 2001—including one claim of 80 overtime hours in a 2-week pay period. However, we were unable to substantiate the claimed hours because, among other

OAS'S PROBLEMS WITH ITS CASH AWARDS PROGRAM REVEAL DEFICIENCY IN DEPARTMENTAL PROCESS

During our OAS review, we found a number of management control weaknesses in the office's administration both of its own cash awards program and that of the Department, which we felt warranted the immediate attention of the Chief Financial Officer and Assistant Secretary for Administration, as they suggested a possible Department-wide problem. In June 2002 we presented these findings to him in a special memorandum:

- Payroll taxes were not withheld from \$24,650 in awards paid to 50 employees because OAS failed to provide the appropriate paperwork to the Office of Human Resources Management (OHRM), and OHRM did not have a process to detect such problems.
- Nine OAS employees received awards that exceeded departmental thresholds—in calendar year 2001, six received more than the \$1,000 limit for Cash-in-Your-Account (CIYA) awards (the awards ranged from \$1,200 to \$1,700); in FY 2001, three received a combination of awards totaling more than the allowable 10 percent of their base pay (in one case, award amounts totaled 30 percent of the employee's base).
- Justification for special act awards was in some cases not provided, in others weak, and in still others did not fit the award criteria.

Our subsequently issued report (IPE-15131) provided the following recommendations to correct these deficiencies: OAS should (1) establish a documented awards process that has a designated manager, an awards tracking mechanism, and a training component on departmental guidelines; (2) institute reconciliation procedures to verify that award amounts are accurate and properly taxed; and (3) develop automated controls to ensure that awards comply with departmental threshold requirements.

The CFO/ASA agreed with these recommendations and has taken appropriate corrective action. The director of the Office of Management Support Services was designated as OAS's incentive awards program officer. OHRM revised the CIYA award policy to require that all cash awards be processed through the Department's payroll service, and that the bureaus develop a tracking system to document the net dollar value of CIYA awards made to individual employees and monitor compliance with the annual \$1,000 CIYA award limitation. OAS will also use its tracking system to ensure that total awards for each employee do not exceed 10 percent of base salary. And, finally, prior to processing CIYA awards, OHRM will conduct a comprehensive technical review of them to verify eligibility and conformance with award procedures and dollar limitations.

Also, in response to our report, the acting director of the Office of Human Resources Management asked Commerce bureaus to examine their awards transactions to determine whether CIYA awards were being properly taxed. By the end of September 2002 it appeared that the failure to withhold taxes from these awards was a problem at four units. Commerce management is working to identify all nontaxed awards and correct the weakness.

things, time and attendance records and overtime authorizations were incomplete or missing. OAS needs to better manage the time and attendance process to ensure that overtime authorizations are properly completed and approved and that timekeepers maintain all documentation for the required period of 6 years. The Department has implemented procedures to ensure that OAS's time and attendance records are better managed.

■ **Energy and environmental programs need attention.**

The Department's Energy Management Program promotes use of renewable energy technologies among the bureaus and helps them reduce energy and water consumption and manage utility costs. The Environmental Management Program helps bureaus comply with environmental legislation. OAS, which administers both programs, has been slow to take action to ensure that the Department is in compliance with applicable laws and regulations pertaining to federal energy and environmental programs.

For example, Commerce's Strategic Implementation Plan for Energy Management contains 70 action items that have not been completed. OAS recently hired an energy management officer, who should be tasked with completing the items and given the staff support and resources to do so. The Department agreed, and has directed the energy manager to help Commerce bureaus address the objectives outlined in the energy management plan.

The environmental program is supposed to coordinate reviews and surveys that require Department-wide response, develop an inventory of Commerce sites that store regulated and/or hazardous materials, perform environmental audits, establish an intra-agency task force on environmental compliance, and provide guidance on environmental regulations and training in meeting their requirements. To date, much of this remains undone. The environmental manager position has been vacant since May 2002, and in the interim, there has been virtually no progress on developing the program. We recommended that OAS fill this position as quickly as possible to ensure compliance with regulations as well as to provide adequate protection for the Department. The Department is in the process of hiring an environmental manager.

Overall, we are very pleased with the prompt attention and action taken in response to the matters we raised in our report. (*OFFICE OF INSPECTIONS AND PROGRAM EVALUATIONS: IPE-15131*)

INFORMATION SECURITY REQUIREMENTS NEED TO BE INCLUDED IN THE DEPARTMENT'S INFORMATION TECHNOLOGY SERVICE CONTRACTS

As the federal workplace has become more dependent on information technology, the government has increased its reliance on outside contractors to perform various IT services. These services may be performed onsite or remotely, from contractors' facilities. In many cases, contractors have access to sensitive information, or, by virtue of the services they perform, may be able to gain such access.

In September 2001 OIG completed an independent evaluation of the Department's information security program, as required by the Government Information Security Reform Act, in which we identified numerous information security weaknesses. Among those deficiencies was the lack of sufficient policy and guidance to ensure that contract documents for IT services contain adequate information security provisions.

During this semiannual period, we followed up on this finding from our earlier report by reviewing the security provisions contained in a sample of the Department's IT service contracts. We found that contract provisions to ensure the safeguarding of sensitive but unclassified systems and information are either missing or inadequate, and that federal guidance for establishing such provisions is minimal and vague.

We made five recommendations aimed at ensuring that all contracting offices within Commerce include adequate information security provisions in IT service contracts and thus protect the Department's sensitive IT information and assets. Essentially, we urged the Department to establish standard contract provisions for safeguarding the security of unclassified systems and to disseminate clear, detailed policy for acquiring these systems and services. Such policy should require that contracting offices, with assistance from information security and program officials, among other things, assess the information security risk associated with the proposed service or system during the acquisition planning phases; identify and include appropriate security requirements in specifications and work statements; monitor contractor performance to ensure compliance with these requirements; and terminate the contractor's access to systems and networks once the contract is closed out. We also advised that the Department should review all current contracts and solicitations for IT services to determine whether information security provisions should be added to them, even though such revisions may increase contract costs, and to ensure that

all procurement personnel receive appropriate training in information security so that they can properly prepare, negotiate, and monitor these contracts.

DEPARTMENT'S RESPONSE

The Department's Chief Financial Office and Assistant Secretary for Administration generally agreed with all of our recommendations and is taking actions to implement them. (*OFFICE OF SYSTEMS EVALUATION: OSE-14788*)

STRONGER MANAGEMENT CONTROLS WERE NEEDED FOR CAMS

The Commerce Administrative Management System—an important effort to improve and unify Department-wide financial management—is expected to be successfully implemented in most Commerce organizations by FY 2004. The exceptions are ITA, USPTO, and NTIS, which will continue to obtain accounting services from other sources. According to the Department's FY 2004 *CAMS Capital Asset Plan*, starting in FY 2004, annual operation and maintenance costs are expected to exceed \$35 million.

In October 2001, funding scenarios under consideration would have significantly reduced CAMS's FY 2002 budget for development and maintenance. The Department believed these funding levels would prevent NOAA from completing its CAMS implementation in FY 2002. Because we were monitoring CAMS's progress, to conduct our own evaluation we requested information that we believed the Department would have needed to determine the impact of the proposed funding level. The Department did not provide all of the information we requested, and based on the information we received, we were not able to determine the likely impact of the proposed funding level.

Plans for CAMS major system activities needed to be improved

At the time of our fieldwork, the CAMS Support Center could not readily provide a detailed plan that specified the cost of all major system activities. The plan it provided for our review at the beginning of FY 2002 accounted for only a portion of these costs and activities. We were informed that by the beginning of FY 2002, the center knew informally how it would spend its funds but we were not provided a complete, documented plan. Notwithstanding the obvious progress made on CAMS recently,

CAMS's history of difficulties and its importance to Commerce's financial management prompted us to recommend that the support center prepare and maintain a plan that (1) specifies full costs for all major system developments and enhancements as well as operations and maintenance activities; and (2) can be substantiated by an analysis of the work required to meet capability and schedule goals. The plan should be updated by the start of the fiscal year to incorporate the most current information about program funding and system activities, including all associated costs. We subsequently received documentation indicating that the CSC has initiated the development of the planning information we initially requested. This documentation will enhance departmental managers' and other stakeholders' management and oversight of CAMS.

The total actual costs of CAMS major system activities needed to be tracked in a more transparent manner

The Clinger-Cohen Act requires executive agencies to measure program progress "in terms of cost, capability of the system to meet specified requirements, timeliness, and quality." Although the center tracked the cost of "contract tasks," until recently, it did not systematically track the total actual cost of major system activities. This approach did not provide the level of information we believe is necessary for effectively evaluating progress. We recommended that the Department take the necessary actions to ensure that the total actual cost of major system activities for CAMS is tracked. After our draft report was issued, we received documentation indicating that the CSC is tracking total actual costs of major system activities.

CAMS reports needed to provide greater visibility into the program

Commerce prepares two types of reports on CAMS spending and progress: (1) The annual *CAMS Capital Asset Plan*, submitted to OMB, is supposed to describe and justify the program; detail its cost, schedule, and capability goals; and report progress in meeting goals; (2) *CAMS Quarterly Reports* are supposed to show progress against the Department's established baseline schedule and cost estimates for major systems activities.

We examined the reports issued in FY 2001 and determined that neither of the reports provided adequate visibility into the program's baseline plans or into the impact of program changes. The Department, we concluded, could improve both reports so that they provide the information needed to better evaluate CAMS program progress.

We specifically recommended that the *Capital Asset Plan* be updated to provide cost estimates that are based on the work to be performed and supported by an appropriate cost-estimating methodology, and to include a comparison of actual progress toward meeting schedule and system capability goals. We further recommended that the *Quarterly Reports* describe the impact of deviations from the baseline on future costs and delivery schedules.

When we met with CSC officials in July, after our draft report was issued, we obtained the quarterly report for the second quarter of FY 2002 and found that it demonstrates some changes consistent with our recommendation. Specifically, the report describes the impact of delays on schedule and users, although it does not address their effect on program costs. The Department believes that additional information is not needed because the report is not intended for the uses we have suggested, but rather to provide summary status information only. We also were given a draft FY 2004 *CAMS Capital Asset Plan*, which included revised fiscal year costs and estimated future costs. A detailed schedule, capability goals, and actual progress information were not included in the material we received.

A performance-based management system should be implemented and maintained

The support center should implement a performance-based management system as soon as possible to support day-to-day CAMS management and comply with OMB requirements. Performance-based management provides objective information about a program's progress to protect against excessive deviations from goals. At the time of our fieldwork, the center had no integrated system for tracking cost, schedule, and capabilities. CSC officials indicated that the center did have a budgetary process for collecting and monitoring schedule, cost, and progress data and that an integrated software system that supports full performance-based management will be implemented.

Summary of Department's Response

In its response to our draft report the Department disagreed with many of our specific findings and indicated it believed it generally had the information needed to manage the CAMS program. However, the Department did subsequently agree that further improvements can be made. (*OFFICE OF SYSTEMS EVALUATION: OSE-14129*)

SECOND DEPARTMENTAL GISRA EVALUATION FINDS PROGRESS MADE, BUT MUCH WORK STILL AHEAD

OIG conducted its second annual evaluation of Commerce's information security program and practices, as mandated by the Government Information Security Reform Act, to determine progress made toward complying with GISRA and any problems that remain. We based our evaluation on the results of security-related OIG reviews we conducted at the Department and its operating units during FY 2002 and on interviews and written materials we received from chief information officers and senior information security officials at the Department and at BIS, ITA, NTIA, and NOAA.

In last year's evaluation we reported that the Department was striving to improve information security and make it an integral component of its business operations, but concluded that because this issue has received inadequate attention in the past, the effort required to develop and oversee an effective security program was substantial. (See September 2001 issue, page 59.) As we recommended, Commerce identified inadequate information technology security controls as a material weakness in its FY 2001 statement on financial and management controls.

This year we noted that the Department has made considerable strides toward establishing the foundation for an effective security program, but numerous weaknesses persist. Most notably, many of the IT systems in the units we evaluated are operating without required risk assessments, approved security plans, or accreditations. Commerce established September 30, 2002, as the deadline for having approved security plans for all operational systems. We believe this schedule is unrealistic for developing high-quality plans, and until all the Department's national-¹⁰ and mission-critical systems are accredited, Commerce should continue to report information security as a material weakness. The Department's FY 2002 GISRA report states that the CIO intends to recommend to the Secretary that information security be repeated as a material weakness.

Despite these serious deficiencies, we found in this year's review that progress has been made on many fronts and that the Department's determination to improve information security continues. Last fiscal year the Secretary directed top management to (1) give information security high priority, sufficient resources, and personal attention; and (2) restructure (and thus strengthen) IT management by having a CIO at each unit who reports to the unit head and the Department CIO, and giving unit CIOs greater authority over IT resources. Action on these directives has fol-

¹⁰ National-critical systems are part of the nation's critical infrastructure.

lowed. Officials at every unit we reviewed are giving this issue their personal attention and taking steps to improve the status of information security. BIS, ITA, and NOAA, for example, are working to ensure that the Department CIO's information security guidance is implemented. BIS reallocated \$500,000 to information security in FY 2002 and ITA devoted \$372,000 in carryover funds. The Department is expanding information security staff at the CIO's office and requires CIO concurrence with IT investment decisions for all major systems. Operating unit CIOs must concur with significant IT investments not subject to departmental approval.

In FY 2001 we noted that the process for identifying the Department's critical assets—those deemed essential to the minimal functioning of the economy—needed to be improved and that Commerce performs too few reviews of unit compliance with government-wide and Department-wide security requirements. Commerce officials responded to these findings in FY 2002 by initiating a Project Matrix review—a process that will identify its critical assets and any public or private systems on which they depend—and by establishing a compliance review process to evaluate all operating unit information security programs and systems over a 3-year cycle.

Revised Department-wide information security policy

In response to our recommendation last year, the Department updated and expanded its information security policy. (As of September 30, 2002, the draft was being circulated for review.) A current and complete policy is essential for establishing an effective Department-wide security program. The new policy will set requirements that are consistent with GISRA guidance and that target a number of deficiencies we identified in our 2001 evaluation and again this year:

- **Incident response procedures.** Last year we found that only 4 of 15 operating units had a formal incident response capability. The draft policy includes guidance on incident identification, handling, response, and reporting. In a related move, the Department established a computer incident response team (CIRT) to give incident response capabilities to units that do not have them.
- **Information security clauses in IT service contracts.** We noted last year a lack of sufficient policy and guidance to ensure that contract documents for IT services contained adequate information security provisions and confirmed the widespread nature of this deficiency in a more extensive review conducted during this semiannual period (see page 51). The Department's draft policy provides specific guidance to protect sensitive systems and information in contracting for IT resources and services.

- **Personnel training.** The policy stipulates that new employees and contractors must receive information security awareness training within 30 days of hire and prior to using any IT resource, and all existing employees and contractors who have access to sensitive systems must have annual refresher training. In the past year the operating units provided security awareness training for all employees and contractor personnel either through programs of their own or via web-based training made available by the CIO. But the policy falls short of adequately addressing the need for appropriate training for personnel with significant information security responsibilities. However, Commerce has formed a working group whose goal is to improve IT security awareness and training Department-wide. As part of its mission the group intends to specify employee functions that require general and specialized training.

The draft policy also directs operating units to maintain a plan for correcting identified information security weaknesses, tracking progress at eliminating them, and reporting monthly to the Department CIO on the status of these efforts.

Persistent weaknesses

The many strides the Department has made—though important—remain somewhat overshadowed by the broad-based lack of adequate information security controls, which prompted our repeat recommendation that Commerce report IT security as a material weakness. GISRA gives senior agency officials responsibility for assessing the information security risks for programs and systems over which they have control, determining the levels of security appropriate to protect associated operations and assets, and periodically testing and evaluating information controls and techniques. The Secretary has charged all operating unit heads with these same responsibilities for their organizations. GISRA also requires the Department's CIO to ensure that effective policies and procedures are implemented for the systems that support the CIO's functions. Operating unit CIOs are expected to do the same.

However, some program officials and operating unit CIOs have yet to fully execute these responsibilities for many of the systems they control. As we have noted, the operating units we reviewed had largely failed to conduct risk assessments on their systems—a prerequisite for developing security plans—despite the Department's September 30 deadline for having approved security plans in place. (See, for example, our findings for NIST, page 39.) Numerous systems were operating without approved security plans or accreditation. We found only one instance of documentation of security control testing—this was for a NOAA system at the Office of Oceanic and Atmospheric Research.

In addition, the reviews of general controls on financial information systems, conducted by outside auditors as part of the audit of Commerce’s FY 2001 financial statements, identified weaknesses pertaining to information security at several bureaus. In general, the corrective action plans for financial systems, if implemented appropriately, will address the weaknesses. In some cases, issues have already been resolved.

Finally, we noted in last year’s evaluation that most FY 2002 capital asset plans failed to identify security costs. Most of the FY 2003 capital asset plans we reviewed this year did specify those costs, but only a few explained how the funds would be spent and several did not detail specific risks and security controls for the life cycle of the system. We concluded that the units should better identify these life-cycle issues so that security expenditures can be better estimated and justified. (*OFFICE OF SYSTEMS EVALUATION: OSE-15260*)

MEMORANDUM NOTES IMPROVEMENTS, REMAINING SAFETY VULNERABILITIES AT COMMERCE HEADQUARTERS BUILDING

In our March 2002 *Semiannual Report to Congress*, we detailed the findings of our safety inspection of selected areas in Commerce headquarters—the Herbert C. Hoover Building—which uncovered a number of potential hazards and vulnerabilities. (See March issue, page 81.) To assess the Department’s response to our corrective recommendations, we conducted another walk-through during this reporting period and were pleased to find that most of the problems we had identified in the basement and subbasement have been resolved. These areas have been cleaned up and are in relatively good order: equipment and furniture have either been removed or stored more appropriately; trash that once littered the floors has been collected and disposed of; chemicals and paint are more carefully stored; and appropriate security devices have been installed on doors and in corridors. The Office of Security reported that it regularly patrols these areas as well.

Only three of our recommendations remain open, including that the Department implement new safety and cleanliness standards for contractors, and provide backup for the Energy Management Computer System. Commerce officials are working to correct these lingering safety and security concerns. We will report on their progress in future semiannual reports.

PREAWARD FINANCIAL ASSISTANCE SCREENING

As part of our ongoing emphasis on prevention of fraud and mismanagement, we continue to work with the Office of Executive Budgeting and Assistance Management, NOAA and NIST grant offices, and EDA program offices to screen the Department’s proposed grants and cooperative agreements before award. Our screening serves two functions: it provides information on whether the applicant has unresolved audit findings and recommendations on earlier awards, and it identifies any negative financial or investigative history on individuals or organizations connected with a proposed award.

During this period we screened 1,132 proposed awards. For 89 of the awards, we found major deficiencies that could affect the ability of the prospective recipients to maintain proper control over federal funds. On the basis of the information we provided, the Department delayed 47 awards until concerns were satisfactorily resolved and established special conditions for 42 awards to adequately safeguard federal funds. (*OFFICE OF AUDITS*)

Preaward Screening Results

Results	Award	
	Number	Amount
Awards delayed to resolve concerns	47	\$29,222,900
Special award conditions established	42	\$24,816,864

NONFEDERAL AUDIT ACTIVITIES

In addition to undergoing OIG-performed audits, certain recipients of Commerce financial assistance are periodically examined by state and local government auditors and by independent public accountants. OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, sets forth the audit requirements for most of these audits. For-profit organizations that receive Advanced Technology Program funds from NIST are audited in accordance with *Government Auditing Standards* and *NIST Program-Specific Audit Guidelines for ATP Cooperative Agreements*, issued by the Department.

We examined 161 audit reports during this semiannual period to determine whether they contained any audit findings related to

Department programs. For 94 of these reports the Department acts as oversight agency and monitors the audited entity’s compliance with the OMB circular or NIST’s program-specific reporting requirements. The other 67 reports are from entities for which other federal agencies have oversight responsibility. We identified a total of 30 reports with findings related to the Department of Commerce.

Report Category	OMB A-133 Audits	ATP Program-Specific Audits	Total
Pending (April 1, 2002)	6	57	63
Received	138	55	193
Examined	102	59	161
Pending (September 30, 2002)	42	53	95

The following table shows a breakdown by bureau of the \$352 million in Commerce funds audited.

Bureau	Funds
EDA	\$ 40,406,093
NIST*	136,727,925
NOAA	15,133,905
NTIA	234,510
Multiagency	157,740,152
Agency not identified	1,972,000
Total	\$352,214,585

* Includes \$107,190,891 in ATP program-specific audits.

The audits identified a total of \$8,479,480 in questioned costs. In most reports the subject programs were not considered major programs; thus the audits involved limited transaction and compliance testing against laws, regulations, and grant terms and conditions. The 30 reports with Commerce findings are listed in Appendix B-1. *(ATLANTA AND DENVER REGIONS’ OFFICE OF AUDITS)*

OIG HIGHLIGHTS: SPECIAL ITEMS OF NOTE

IGs FRAZIER, REHNQUIST, AND FRIEDMAN TESTIFY BEFORE CONGRESSIONAL COMMITTEE ON PURCHASE CARD OVERSIGHT

On May 1, 2002, Inspectors General Johnnie Frazier, Janet Rehnquist, and Gregory Friedman testified about oversight of the purchase card programs at Commerce, HHS, and Energy, respectively, before the U.S. House of Representatives' Subcommittee on Oversight and Investigations, Committee on Energy and Commerce. In the past year, intense congressional and media scrutiny of the government's purchase card program tended to focus on past abuses. In April 2002 the OMB director requested that each agency review the adequacy of internal controls for purchase and travel card expenditures and prepare separate remedial purchase and travel card program action plans by June 2002. OMB subsequently asked agency leaders to provide quarterly reports on their program improvement plans.

During his testimony, IG Frazier shared with the subcommittee some of "the good, the bad, and the ugly" things our reviews revealed about Commerce's program.

- **The good:** The overwhelming number of Commerce and other federal employees use their government purchase cards responsibly—following appropriate procedures, avoiding improper purchases, and staying alert to best practices that can help the program operate efficiently.
- **The bad:** The program still has a number of systemic weaknesses and problematic practices that needlessly leave it open to fraud, waste, and abuse.
- **The ugly:** Reports in the media and from OIGs and other oversight organizations have highlighted irresponsible and illegal use of government purchase cards, and as a result have given the purchase card program a negative image.

Mr. Frazier noted that government employees have relied on purchase cards for more than 15 years to expedite making small purchases, obtain training, and otherwise streamline unwieldy federal procurement procedures. As Commerce and other agencies push for greater efficiency in the process, purchase cards will

become an evermore critical procurement option and their use will inevitably increase. Mr. Frazier suggested that improving the purchase card program government-wide must be guided by three key principles:

- **Stop** any and all personal use of government cards with aggressive oversight and strong disciplinary actions.
- **Caution** managers to address systemic weaknesses and problematic practices.
- **Go** forward at full speed to implement best practices and other proactive efforts that will prevent problems and promote efficiencies.



IGs Frazier, Friedman, and Rehnquist being sworn in to testify before the congressional Committee on Purchase Card Oversight.

In 1995 this office began conducting audits and reviews of purchase card use and related activities within the Department. Since then we have issued 11 audit reports dealing specifically with the purchase card program. Our audits included headquarters operations at MBDA, NTIA, and USPTO, as well as overseas posts, certain NIST laboratories, NOAA science centers, and regional offices. Our primary objective was to determine whether purchase card use was in compliance with the Federal Acquisition Regulation, the *Commerce Acquisition Manual*, and the Department's *Personal Property Management Manual*.

We also covered purchase card use in a number of inspection reports as part of overall reviews of administrative services at the

offices inspected. We have found that these proactive reviews are especially useful in identifying systemic weaknesses in internal controls designed to safeguard the program.

We are conducting a Department-wide audit of the purchase card program in accordance with our audit goals for 2002-2003. Based on our reviews, we believe the vast majority of Commerce's 6,000 cardholders are using the cards responsibly and adhering to guidelines. We also know that our work, along with that of Commerce officials and managers, must continue as we look for ways to improve the program and implement best practices to resolve problems, prevent and detect fraud, and encourage efficiencies. A number of proactive efforts deserve special emphasis:

- Properly train and support approving officials and cardholders.
- Publicize common problems and their solutions.
- Look for problems before the problems find you.
- Maintain sufficient and constant oversight.

The Subcommittee on Oversight and Investigations plans to hold additional hearings this spring, as do other oversight committees, signifying a continued high level of congressional interest.

THE PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY

The President's Council on Integrity and Efficiency (PCIE), comprised of the presidentially appointed inspectors general, was established to address integrity, economy, and effectiveness issues that transcend individual government agencies and to increase the professionalism and effectiveness of IG personnel throughout the government. To accomplish their mission, PCIE members meet regularly to address concerns pertinent to their oversight responsibilities. They also conduct interagency audits, inspections, and investigations to prevent fraud, waste, and abuse and promote economy and efficiency in federal programs and operations. By combining their efforts, they are able to more effectively address government-wide issues of fraud, waste, and abuse as well as inefficiency and ineffective management. Council members also develop policies, standards, and approaches to aid in establishing a well-trained and highly skilled IG workforce.

Commerce Inspector General Johnnie Frazier is a member of the PCIE and chair of the PCIE Inspection and Evaluation Committee.

INSPECTION AND EVALUATION COMMITTEE

A primary function of the Inspection and Evaluation (I&E) Committee is to share and develop better ways to communicate inspection and evaluation findings on crosscutting issues. The goals of the PCIE Inspection and Evaluation Committee are to

- provide positive contributions to the inspector general community as well as the federal government as a whole in improving the management of federal programs;
- improve the methodologies of inspection and evaluation by sharing effective practices and insights; and
- improve the analytic and administrative skills of OIG inspectors and evaluators by providing training in a variety of pertinent topics.

Recently, building on the work of the OIGs at Education, Commerce, and other agencies, the committee completed its purchase card project with the publication of *A Practical Guide for Reviewing Government Purchase Card Programs* (see below). The committee developed and published the report as an adjunct to individual agency purchase card review programs, to aid the IG community in addressing the increasingly important issue of purchase card use and abuse.

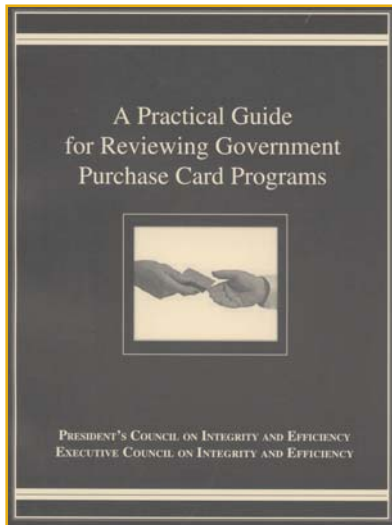
Other important issues—emergency preparedness, the status of foreign nationals working for government agencies, procurement and acquisitions—are concerns all or several OIGs must grapple with and have been offered as future project areas. The committee proposes projects to the PCIE and develops procedures and methodologies to achieve project goals.

A PRACTICAL GUIDE FOR REVIEWING GOVERNMENT PURCHASE CARD PROGRAMS

In June this office published PCIE's *A Practical Guide for Reviewing Government Purchase Card Programs*, a collaborative effort with the Department of Education OIG and several other Offices of Inspector General. It is a helpful addition to the growing number of tools federal IGs have already developed to use in overseeing purchase card activities in their agencies.

Government-wide, purchase cardholders spent \$13.7 billion in FY 2001—a 12 percent increase over the previous year. This timely guide has been a high priority for the I&E Committee

because of its focus on so critical an area for IG review. Much effort went into making this document a useful reference tool for all PCIE members as well as others who oversee or manage purchase card activities. Staff at the Department of Education OIG took the lead in developing this project but the effort was truly a collaborative one. The purchase card guide will help IGs more effectively focus their efforts and serves as yet another example of the commitment of the inspectors general to work collectively to promote efficiency and effectiveness throughout the federal government.



The guide is intended to supplement existing federal law, regulations, and internal agency guidelines and to be used in conjunction with other audit, inspection, or investigative tools. But *A Practical Guide for Reviewing Government Purchase Card Programs* also provides commonsense advice based on experience and includes practical features to aid in the review process such as questionnaires

and templates. In addition, the guide contains a multiagency resource list of OIG reviews, providing examples of how different agencies—including Agriculture, Commerce, Education, Energy, GSA, Interior, State, Transportation, and VA OIGs and GAO—conduct and present reviews of the purchase card program. It comes at a most opportune time as many IG offices continue their important work in this critical area.

SPECIAL AWARDS

2002 PCIE AWARDS FOR EXCELLENCE

Each year, PCIE surveys the work of the IG community and honors particularly outstanding efforts that singularly or collectively advance the council's mission. This year 27 members of our staff and one entire office were honored. In every case, their efforts enhance the entire OIG's reputation for commitment to excellence and exemplify the professionalism and rewards inherent in true teamwork. Recognition is accorded as follows:

Census 2000 Report, *Improving Our Measure of America: What Census 2000 Can Teach us in Planning for 2010*: Chuck Tegeler, Lisa Pearson, Heidi Alves, Jill Haflich, Patricia Derr, Karen DePerini, and Rita Dettmar—for their landmark work in providing timely and critical guidance for improving future decennial operations.

Emergency Preparedness and Physical Security Inspection: Lisa Parker, Sharon Seymore, and former employees Erika Lang, Tim Crowe, Nellie Wild, Peter Han, and Jon Shifrin—for their comprehensive and timely review of emergency preparedness and physical security at 27 Commerce facilities, which revealed a number of troubling weaknesses that needed to be rectified.

False Claims: Allison Lerner, Greg Sebben, and Daniel Buchtel—for their handling of an investigation into fraudulent claims by the recipient of an Advanced Technology Program award that resulted in a significant financial settlement in the Department's favor.

Grants and Cooperative Agreement Manual: Bill Bedwell, Jerry McMahan, Thelma Amos, Kathleen McKeivitt, and Belinda Riley—for their role in developing the *Grants and Cooperative Agreement Manual*, which has greatly enhanced financial and operational soundness in the Department's financial assistance programs.

Interagency Teams

September 11 Response: Ken Clair, James Blake, Robert Brent, and George Chiamulera, who, along with special agents from other agency OIGs, voluntarily participated in recovery, investigative, and security operations related to the terrorist attacks in New York and Washington.

PCIE Purchase Card Guide: Irene Lewkowicz, Belinda Robinson, and the Office of Inspections and Program Evaluations, along with members of the Department of Education OIG—for development, design, and production of *A Practical Guide for Reviewing Purchase Card Programs*.

Special Recognition

George Grob, who recently concluded a 9-year tenure as chair of the Inspections and Evaluation Roundtable, an adjunct to the I&E Committee, received the Individual Achievement Award for his outstanding leadership and the roundtable's significant accomplishments under his watch. Mr. Grob was nominated for this award by the I&E Committee, chaired by IG Frazier.

PRESIDENTIAL MERITORIOUS RANK AWARD

Each year, the President recognizes a small group of career senior executives with the President's Rank Award for exceptional long-term accomplishments. Winners of this award are chosen through a rigorous selection process—nominated by their agency heads, evaluated by boards of private citizens, and approved by the President. This year, Judith Gordon of this office was honored with this prestigious award.

Judith Gordon, Assistant Inspector General for Systems Evaluation, is responsible for planning, managing, and providing technical contributions to a work program that evaluates and actively promotes improvements in the design, acquisition, development, management, and security of the many complex computer systems and related information technology investments throughout the Department.

Ms. Gordon was instrumental in forging an important role for OIGs in overseeing and evaluating information technology investments in the federal government. Recognizing both the importance and increasing complexity of information technology at the Department, Ms. Gordon provided the concept and leadership for establishing OIG's Office of Systems Evaluation in 1994. The systems evaluation capability she introduced to OIG and the Department was unique in government and demonstrated that OIGs have and must play a critical role in ensuring maximum performance in the critical, costly, and problem-prone area of information technology. The oversight program Ms. Gordon leads has also promoted improvements in the development, acquisition, and management of information technology throughout Commerce, including for the 2000 Decennial Census, USPTO, and National Weather Service.

Ms. Gordon's ability to define critical issues and develop practical, constructive solutions for resolving them has earned her widespread admiration and respect throughout the Department and the federal government. In addition to being a crucial source of independent review and recommendations for improving systems acquisition, Ms. Gordon and her staff are also an extremely valuable resource for advice and consultation on technical and

acquisition management issues. A recognized expert in the field of federal information systems management, she is frequently invited to represent OIG as a speaker at conferences and meetings. Articles about her work have appeared in the *Federal Times*, *Government Computer News*, *Federal Computer Week*, and other publications.

COMMERCE'S SILVER MEDAL AWARD

The Silver Medal is one of the highest honors bestowed by the Secretary of Commerce, given to those select few employees whose exemplary achievements have directly enhanced departmental operations. Allen Crawley and Kenneth Clair are OIG's two most recent recipients of this award.

Allen Crawley, Deputy Assistant Inspector General for Systems Evaluation, was recognized for the key role he played in establishing OIG's information security evaluation capability, a highly effective method for assessing the security of the Department's critical information assets. With his guidance, OIG's systems evaluation staff successfully implemented a protocol that identifies and offers solutions for IT security issues, greatly enhancing the Department's efforts to protect its many critical information assets. The program has had a positive impact on every information security program and system assessed. Mr. Crawley's capability and professionalism are well respected by his peers both in OIG and throughout the government.

Special Agent Kenneth Clair, selected on the basis of his work ethic, attitude, and skills, served as a Federal Air Marshal with the Federal Aviation Administration from October 2001 through March 2002. Because of the terrorist incidents on September 11, 2001, the FAA augmented the Federal Air Marshal program with law enforcement officers from other federal agencies until the positions could be staffed with full-time employees. The FAA Federal Air Marshal program is integral to assuring the safety of the flying public by preventing and thwarting hijackings and terrorist attacks on U.S. civilian aircraft.

TABLES AND STATISTICS

STATISTICAL OVERVIEW

AUDIT RESOLUTION AND FOLLOW-UP

The Inspector General Act Amendments of 1988 require us to present in this report those audits issued before the beginning of the reporting period (April 1, 2002) for which no management decision had been made by the end of the period (September 30, 2002). One NOAA audit report remains unresolved for this reporting period.

Department Administrative Order 213-5, Audit Resolution and Follow-up, provides procedures for management to request a modification to an approved audit action plan or for a financial assistance recipient to appeal an audit resolution determination. The following table summarizes modification and appeal activity during the reporting period.

Audit Resolution Follow-Up

Report Category	Modifications	Appeals
Actions pending (April 1, 2002)	0	6
Submissions	0	6
Decisions	0	4
Actions pending (September 30, 2002)	0	8

Audit and Inspection Statistical Highlights for this Period

Questioned costs	\$11,885,325
Value of audit recommendations that funds be put to better use	\$11,167,739
Value of audit recommendations agreed to by management	\$9,198,142
Value of inspection recommendations that funds be put to better use	\$0

INVESTIGATIVE OPERATIONS AND STATISTICS

The Office of Investigations (OI) has authority to investigate alleged or suspected fraud, waste, abuse, or mismanagement by Department of Commerce employees, contractors, recipients of financial assistance, and others involved in the Department's programs and operations. These investigations typically result in criminal and/or civil prosecution, as well as administrative sanctions for violation of Department regulations and employee standards of conduct.

OI is composed of special agents and support staff strategically located in Atlanta, Georgia; Denver, Colorado; Silver Spring, Maryland; and Washington, D.C. OI special agents are deputized as special deputy U.S. marshals pursuant to a memorandum of understanding (MOU) with the Department of Justice and the Federal Bureau of Investigation. This MOU provides all special agents with full law enforcement authority while engaged in the performance of their duties, including the authority to carry a firearm, make arrests, and execute search warrants.

During the past 6 months OI has conducted outreach within Commerce that focused on informing and educating Department personnel to recognize and report suspected fraudulent activity related to their specific programs. OI is also beginning to proactively pursue issues that may be appropriate for investigation or referral to a cognizant office or bureau. This approach is designed to enhance our ability to prevent and detect fraud and will allow us to identify potential vulnerabilities in Department programs and operations. In addition, OI is continuing to partner with the various operating units in both Commerce and OIG to ferret out fraud and address systemic problems that impede the efficacy of departmental programs.

Investigative Statistical Highlights for this Period

Investigative Activities	
Cases opened	63
Cases closed	45
Complaints received	130
Criminal Investigative Activities	
Indictments/informations	3
Convictions	3
Sentencings	3
Jail	6 1/2 mos.
Probation/supervised release	132 mos.
Criminal judgments/restitutions/fines	\$42,687
Criminal matters referred for prosecution	14
Criminal matters accepted for prosecution	11
Criminal matters declined	3
Civil Investigative Activities	
Civil matters referred for prosecution	2
Civil matters accepted for prosecution	1
Civil matters declined for prosecution	1
Civil recoveries in dollars (minimum amount, to be paid over time)	\$700,000
Administrative Investigative Activities	
Matters referred for administrative action	20
Employee suspensions	1
Reprimands/counseling	1
Other personnel actions	1
Downgrades	1
Procurement remedies	1
General policy actions	4

REPORTING REQUIREMENTS

Index

The Inspector General Act of 1978, as amended (1988), specifies reporting requirements for semiannual reports. The requirements are listed below and indexed to the applicable pages of this report.

Section	Topic	Page
4(a)(2)	Review of Legislation and Regulations	62
5(a)(1)	Significant Problems, Abuses, and Deficiencies	14-56
5(a)(2)	Significant Recommendations for Corrective Action	14-56
5(a)(3)	Prior Significant Recommendations Unimplemented	63
5(a)4	Matters Referred to Prosecutive Authorities	14-56
5(a)(5) and 6(b)(2)	Information or Assistance Refused	63
5(a)(6)	Listing of Audit Reports	64-69
5(a)(7)	Summary of Significant Reports	14-56
5(a)(8)	Audit Reports—Questioned Costs	64
5(a)(9)	Audit Reports—Funds to Be Put to Better Use	65
5(a)(10)	Prior Audit Reports Unresolved	61
5(a)(11)	Significant Revised Management Decisions	63
5(a)(12)	Significant Management Decisions with which OIG Disagreed	63

OIG is also required by section 804(b) of the Federal Financial Management Improvement Act of 1996 to report on instances and reasons when an agency has not met the dates of its remediation plan. We discuss this matter in the March 2003 issue as part of our financial statements audit reporting.

4(a)(2): REVIEW OF LEGISLATION AND REGULATIONS

This section requires the inspector general of each agency to review existing and proposed legislation and regulations relating to that agency’s programs and operations. Based on this review, the inspector general is required to make recommendations in the

semiannual report concerning the impact of such legislation or regulations on the economy and efficiency of the management of programs and operations administered or financed by the agency or on the prevention and detection of fraud and abuse in those programs and operations. Comments concerning legislative and regulatory initiatives affecting Commerce programs are discussed, as appropriate, in relevant sections of the report.

SECTION 5(a)(3): PRIOR SIGNIFICANT RECOMMENDATIONS UNIMPLEMENTED

This section requires identification of each significant recommendation described in previous semiannual reports for which corrective action has not been completed. Section 5(b) requires that the Secretary transmit to Congress statistical tables showing the number and value of audit reports for which no final action has been taken, plus an explanation of the reasons why recommended action has not occurred, except when the management decision was made within the preceding year.

To include a list of all significant unimplemented recommendations in this report would be duplicative, costly, unwieldy, and of limited value to Congress. Any list would have meaning only if explanations detailed whether adequate progress is being made to implement each agreed-upon corrective action. As this semiannual report was being prepared, management was in the process of updating the Department's Audit Tracking System as of September 30, 2002, based on annual status reports due from the bureaus in mid-October. An accurate database was therefore not available to OIG for reference here. However, additional information on the status of any audit recommendations can be obtained through OIG's Office of Audits.

SECTIONS 5(a)(5) AND 6(b)(2): INFORMATION OR ASSISTANCE REFUSED

These sections require a summary of each report to the Secretary when access, information, or assistance has been unreasonably refused or not provided. There were no such instances during this semiannual period and no reports to the Secretary.

SECTION 5(a)(10): PRIOR AUDIT REPORTS UNRESOLVED

This section requires a summary of each audit report issued before the beginning of the reporting period for which no man-

agement decision has been made by the end of the reporting period (including the date and title of each such report), an explanation of why a decision has not been made, and a statement concerning the desired timetable for delivering a decision on each such report.

As of September 30, 2002, the following single audit summary relating to a NOAA grant was unresolved for more than 6 months:

Questioned Costs for North Pacific Marine Science Foundation (Washington) Total \$177,527

An OIG desk review of this NOAA single audit report (listed in our March 2002 issue, page 111, ATL-09999-2-0430) questioned a total of \$177,527 in relation to undocumented in-kind contributions, unapproved indirect costs, costs claimed that were excessive because an incorrect exchange rate was used for conversion, undocumented costs on federal reports, duplicate costs claimed for federal reports, and unallowable travel. The report also contained some nonfinancial findings. NOAA has not yet submitted to OIG an audit resolution proposal for this report.

SECTION 5(a)(11): SIGNIFICANT REVISED MANAGEMENT DECISIONS

This section requires an explanation of the reasons for any significant revision to a management decision made during the reporting period. Department Administrative Order 213-5, Audit Resolution and Follow-up, provides procedures for revising a management decision. For performance audits, OIG must be consulted and must approve in advance any modification to an audit action plan. For financial assistance audits, OIG must concur with any decision that would change the audit resolution proposal in response to an appeal by the recipient. The decisions issued on the four appeals of audit-related debts were finalized with the full participation and concurrence of OIG.

SECTION 5(a)(12): SIGNIFICANT MANAGEMENT DECISIONS WITH WHICH OIG DISAGREED

This section requires information concerning any significant management decision with which the inspector general disagrees. Department Administrative Order 213-5 provides procedures for elevating unresolved audit recommendations to higher levels of Department and OIG management, including their consideration by an Audit Resolution Council. During this period no audit issues were referred to the council.

TABLES AND APPENDIXES

TABLES	PAGE
1. Audits with questioned costs	64
2. Audits with recommendations that funds be put to better use	65
APPENDIXES	
A. Report types this period	65
A-1. Performance audits	65
A-2. Financial-related audits	66
A-3. Inspections and Systems Evaluations	67
B. Processed reports	68
B-1. Processed financial-related audits	69

Definitions of Terms Used in the Tables

Questioned cost: a cost that is questioned by OIG because of (1) an alleged violation of a provision of a law, regulation, contract, grant, cooperative agreement, or other agreement or document

governing the expenditure of funds; (2) a finding that, at the time of the audit, such cost is not supported by adequate documentation; or (3) a finding that an expenditure of funds for the intended purpose is unnecessary or unreasonable.

Unsupported cost: a cost that, at the time of the audit, is not supported by adequate documentation. Questioned costs include unsupported costs.

Recommendation that funds be put to better use: a recommendation by OIG that funds could be used more efficiently if Commerce management took action to implement and complete the recommendation, including (1) reductions in outlays; (2) deobligation of funds from programs or operations; (3) withdrawal of interest subsidy costs on loans or loan guarantees, insurance, or bonds; (4) costs not incurred by implementing recommended improvements related to Commerce, a contractor, or a grantee; (5) avoidance of unnecessary expenditures identified in preaward reviews of contracts or grant agreements; or (6) any other savings specifically identified.

Management decision: management’s evaluation of the findings and recommendations included in the audit report and the issuance of a final decision by management concerning its response.

Table 1. Audits with Questioned Costs

Report Category	Number	Questioned Costs	Unsupported Costs
A. Reports for which no management decision had been made by the beginning of the reporting period	28	\$ 4,759,762	\$ 799,192
B. Reports issued during the reporting period	35	11,885,325	4,858,281
Total reports (A+B) requiring a management decision during the reporting period ¹	63	16,645,087	5,657,473
C. Reports for which a management decision was made during the reporting period ²	33	5,902,996	915,432
i. Value of disallowed costs		3,269,494	293,653
ii. Value of costs not disallowed		3,151,167	631,528
D. Reports for which no management decision had been made by the end of the reporting period	30	\$10,742,091	\$4,742,041

¹ Eleven audit reports included in this table are also included among reports with recommendations that funds be put to better use (see table 2). However, the dollar amounts do not overlap.

² In Category C, lines i and ii do not always equal the total on line C because resolution may result in values greater than the original recommendations.

Table 2. Audits with Recommendations That Funds Be Put to Better Use

Report Category	Number	Value
A. Reports for which no management decision had been made by the beginning of the reporting period	6	\$ 1,177,145
B. Reports issued during the reporting period	12	11,167,739
Total reports (A+B) requiring a management decision during the reporting period ¹	18	12,344,884
C. Reports for which a management decision was made during the reporting period ²	10	2,440,055
i. Value of recommendations agreed to by management		5,928,648
ii. Value of recommendations not agreed to by management		180,196
D. Reports for which no management decision had been made by the end of the reporting period	10	\$ 9,904,829

¹Eleven audit reports included in this table are also included in the reports with questioned cost (see table 1). However, the dollar amounts do not overlap.

²In Category C, two reports had funds to be put to better use identified during the resolution process. Also, in Category C, lines i and ii do not always equal the total on line C because resolution may result in values greater than the original recommendations.

Appendix A. Report Types this Period

Type	Number	Appendix
Performance audits	3	A-1
Financial-related audits	19	A-2
Inspections and Systems Evaluations	9	A-3
Total	31	

Appendix A-1. Performance Audits

Agency	Date Issued	Report Title	Report Number	Funds to Be Put to Better Use
NOAA	06/28/02	Program for Acquiring Fisheries Research Vessels Needs Stronger Management Controls	STD-14428-2-0001	–
NOAA	09/30/02	Internal Controls for Travel Cards at OAR's Environmental Technology Laboratory Can Be Strengthened	BTD-14908-2-0001	–
NOAA	09/30/02	Northwest Fisheries Science Center Needs Improved Research Management Processes to Better Implement Its Salmon Research Plan	STD-14440-2-0001	–

Appendix A-2. Financial-Related Audits

Agency/Auditee	Report Number	Date Issued	Questioned Costs	Unsupported Costs	Funds to Be Put to Better Use
EDA					
Eastern Oklahoma Development District	ATL-14301-2-0002	07/18/02			\$300,000
Detroit Economic Growth Corporation, MI	DEN-14963-2-0001	07/22/02			\$749,430
City of East Cleveland, OH	DEN-14962-2-0001	07/31/02			\$513,480
Northwest Arkansas Economic Development District, Inc.	DEN-15019-2-0001	08/28/02			\$400,899
Philadelphia Authority for Industrial Development, PA	ATL-15123-2-0001	08/30/02			\$521,743
East Arkansas Planning and Development District	DEN-14884-2-0001	08/30/02			\$808,229
City of New York	ATL-15125-2-0001	09/05/02	\$57,977	\$57,977	\$3,457,049
City of Seattle, WA	STL-14837-2-0001	09/05/02			\$1,067,265
U.S. Virgin Islands	ATL-15126-2-0001	09/23/02			\$974,378
City of Milwaukee, WI	DEN-14885-2-0001	09/30/02			\$1,492,626
City of Los Angeles, CA— Audit of Three EDA Grants for ACBOP	STL-14900-2-0002	09/30/02	\$97,897	\$28,682	
MBDA					
City of Los Angeles, CA— Audit of the MBDA Award for the LAMBOC	STL-14900-2-0001	09/30/02	\$499,746	\$120,647	
NIST					
TriQuint Semiconductor Texas, Inc., TX	DEN-14517-2-0001	07/08/02			
Minnesota Technology, Inc., MN	DEN-14879-2-0001	07/22/02	\$813,631	\$813,631	\$652,334
Facilichem, Inc., CA	DEN-14886-2-0001	09/12/02	\$483,065		
H Power Corporation, NJ	DEN-14978-2-0001	09/13/02	\$181,819		\$230,306
BioTrove, Inc., MA	DEN-14989-2-0001	09/18/02			
Allegheny-Singer Research Institute, PA	ATL-13993-2-0001	09/26/02	\$843,015	\$435,988	
NOAA					
Pacific States Marine Fisheries Commission, OR	STL-14956-2-0001	09/30/02	\$428,695	\$255,616	

Appendix A-3. Inspections and Systems Evaluations

Agency	Date Issued	Report Title	Report Number	Funds to Be Put to Better Use
BIS	09/30/02	Annual Follow-Up Report on Previous Export Control Recommendations, as Mandated by the National Defense Authorization Act for Fiscal Year 2000, as Amended	IPE-15290	–
NOAA	09/30/02	NWS Weather Forecast Offices Generally Perform Well, but Regional Oversight and Management at Some Offices Need to Be Improved	IPE-14577	–
O/S	04/23/02	Stronger Management Controls Will Improve Planning and Control of CAMS	OSE-14129	–
O/S	05/15/02	Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts	OSE-14788	–
O/S	09/30/02	The Office of Administrative Services Needs Stronger Internal Controls and Management Oversight	IPE-15131	–
O/S	09/30/02	Independent Evaluation of the Department's Information Security Program Under the Government Information Security Reform Act	OSE-15260	–
TA/NIST	09/16/02	Additional Improvements Needed to Strengthen NIST's Information Security Program	OSE-15078	–
USPTO	08/22/02	Stronger Management Controls Needed for Patent Application Capture and Review Automated Information System	OSE-14926	–
USPTO	09/30/02	Independent Evaluation of USPTO's Information Security Program	OSE-15250	–

Appendix B. Processed Reports

The Office of Inspector General reviewed and accepted 161 financial-related audit reports prepared by independent public accountants and local, state, and other federal auditors. The reports processed with questioned costs, recommendations that funds be put to better use, and/or nonfinancial recommendations are listed in Appendix B-1.

Agency	Audits
Economic Development Administration	44
National Institute of Standards and Technology	71*
National Oceanic and Atmospheric Administration	8
National Telecommunications and Information Administration	2
Multiagency	34
Agency not identified	2
Total	161

*Includes 59 ATP program-specific audits.

Appendix B-1. Processed Financial-Related Audits

Agency/Auditee	Report Number	Date Issued	Questioned Costs	Unsupported Costs
EDA				
City of Columbia, SC	ATL-09999-2-1123	09/26/02	\$1,008,942	
City of Watertown, NY	ATL-09999-2-1149	09/30/02	\$706,566	
City of Rio Vista, CA	ATL-09999-2-1194	09/30/02	\$788,838	\$788,838
Macon County, MO	ATL-09999-2-1222	09/30/02	\$466,800	
NIST				
Vitria Technology, Inc., CA	ATL-09999-2-0989	04/09/02	\$191,349	
ETEC Systems Inc., CA	ATL-09999-2-1066	04/09/02	\$17,328	
Caterpillar Inc., IL	DEN-09999-2-0739	04/10/02	\$207,782	\$34,488
U.S. Steel, PA	DEN-09999-2-0698	04/18/02		
The Budd Company, MI	DEN-09999-2-0704	04/18/02		
E.I. DuPont de Nemours, DE	DEN-09999-2-0741	04/18/02	\$245,540	\$70,673
Electro Scientific Industries, Inc., OR	ATL-09999-2-1063	04/19/02	\$13,405	\$13,405
Ebert Composites Corporation, CA	ATL-09999-2-1065	04/19/02	\$15,944	
DaimlerChrysler Corporation, MI	DEN-09999-2-0696	05/03/02		
Eastman Chemical Company, TN	DEN-09999-2-0828	05/23/02	\$4,062	
Walter Juda Associates, Inc., MA	DEN-09999-2-0949	05/23/02	\$10,041	
Chevron Research and Technology Center, CA	DEN-09999-2-0816	06/19/02	\$111,975	
CoorsTek, Inc., CO	DEN-09999-2-0871	06/19/02	\$131,621	\$131,621
Sun Microsystems, Inc., CA	ATL-09999-2-0859	06/24/02	\$17,437	
Synquiry Technologies, Ltd., MA	ATL-09999-2-1198	07/28/02	\$28,782	
Saginaw Machine Systems, Inc., MI	DEN-09999-2-0784	07/30/02	\$21,300	
Imaging Therapeutics, Inc., CA (formerly OsteoNet Com, Inc.)	DEN-09999-2-1081	08/14/02	\$39,972	
VitalWorks, Inc., CT	ATL-09999-2-0982	08/26/02	1,404,505	\$1,404,505
KLA-Tencor Corporation, CA	DEN-09999-2-1238	08/28/02	\$1,632,747	
State of Nebraska	ATL-09999-2-1114	09/12/02	\$616,611	\$616,611
Florida Manufacturing Technology Center	ATL-09999-2-1154	09/12/02	\$167,928	\$20,192
Chicago Manufacturing Center, IL	ATL-09999-2-0630	09/25/02	\$14,689	
Chicago Manufacturing Center, IL	ATL-09999-2-0818	09/25/02	\$1,928	
Chicago Manufacturing Center, IL	ATL-09999-2-1074	09/25/02	\$480,756	\$19,611
3M Company, MN	ATL-09999-2-1192	09/25/02	\$101,382	\$45,796
NOAA				
State of Connecticut	ATL-09999-2-1099	09/20/02	\$31,250	

ACRONYMS

ACBOP	Alameda Corridor Business Outreach Program
ATP	Advanced Technology Program
BEA	Bureau of Economic Analysis
BIS	Bureau of Industry and Security (formerly Bureau of Export Administration)
CAMS	Commerce Administrative Management System
CFIUS	Committee on Foreign Investment in the United States
CFO/ASA	Chief Financial Officer and Assistant Secretary for Administration
CIO	chief information officer
CIRT	computer incident response team
CIYA	Cash-in-Your-Account
CCL	Commerce Control List
COOP	continuity of operations plans
COTR	contracting officers' technical representative
CSC	CAMS Support Center
DOT	U.S. Department of Transportation
ECASS	Export Control Automated Support System
EDA	Economic Development Administration
EEZ	exclusive economic zone
ESA	Economics and Statistics Administration
ETL	Environmental Technology Laboratory
FAR	Federal Acquisition Regulation
FRV	fisheries research vessel
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GPRA	Government Performance and Results Act
GSA	General Services Administration
GWAC	government-wide agency contract
IA	Import Administration
IG	inspector general

IT	information technology
ITA	International Trade Administration
ITL	Information Technology Laboratory
LAMBOC	Los Angeles Minority Business Opportunity Committee
LTED	Long-Term Economic Deterioration
MASC	Mountain Administrative Support Center
MBOC	Minority Business Opportunity Committee
MEP	Manufacturing Extension Partnership
MOU	memorandum of understanding
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NMFS	National Marine Fisheries Service
NOAA	National Oceanic and Atmospheric Administration
NRFU	nonresponse follow-up
NTIA	National Telecommunications and Information Administration
NTIS	National Technical Information Service
NWS	National Weather Service
OAM	Office of Acquisition Management
OAS	Office of the Secretary
OEAM	Office of Executive Assistance Management
OEP	Occupant Emergency Plans
OFPP	Office of Federal Procurement Policy
OHRM	Office of Human Resources Management
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
PACR	Patent Application Capture and Review System
PWP	Public Works Program
RLF	revolving loan fund
SSED	Sudden and Severe Economic Dislocation
US&FCS	U.S. and Foreign Commercial Service
USPTO	U.S. Patent and Trademark Office
WFO	weather forecast office

TYPES OF OIG REVIEWS

For the federal government, OIGs must ascertain program viability from a variety of perspectives. The various kinds of audits, evaluations, inspections, and investigations at our disposal afford the IG's office a comprehensive view of Commerce programs and operations. Thus we are able to provide program managers with reviews and recommendations that are both objective and inclusive and can be used to aid them in ensuring the most efficient and effective use of taxpayer dollars.

AUDITS

Performance Audits address the efficiency, effectiveness, and economy of the Department's programs, activities, and information technology systems. They may check a unit's compliance with laws and regulations, and evaluate its success in achieving program objectives.

Financial-Related Audits review the Department's contracts, grants, cooperative agreements, loans, and loan guarantees. They assess compliance with laws, regulations, and award terms; adequacy of accounting systems and internal controls; allowance of costs; and the degree to which projects achieved the intended results.

Financial Statements Audits determine whether (1) a reporting entity's financial statements are presented fairly and in accordance with generally accepted accounting principles; (2) the entity has an internal control structure that provides reasonable assurance of achieving the control objectives set forth by OMB; and (3) the entity complied with laws and regulations that could have a direct and material effect on the financial statements, the Federal Financial Management Improvement Act, and other laws and regulations.

INSPECTIONS

Inspections are reviews of an activity, unit, or office, or a contractor or other nonfederal entity that receives funds from the Department. They focus on an organization, not a whole program, and are often designed to give agency managers timely and useful information about operations, including current and foreseeable problems.

EVALUATIONS

Program Evaluations are in-depth reviews of specific management issues, policies, or programs.

Systems Evaluations review system development, acquisitions, operations, and policy, focusing on computer systems and other technologies.

INVESTIGATIONS

Criminal/Civil/Administrative Investigations are conducted based on alleged or suspected wrongdoing by Department employees, contractors, recipients of financial assistance, and others responsible for handling federal resources. Investigations that expose violation of Department rules and regulations or acts of fraud committed against the U.S. government can result in administrative sanctions and/or criminal or civil prosecution.