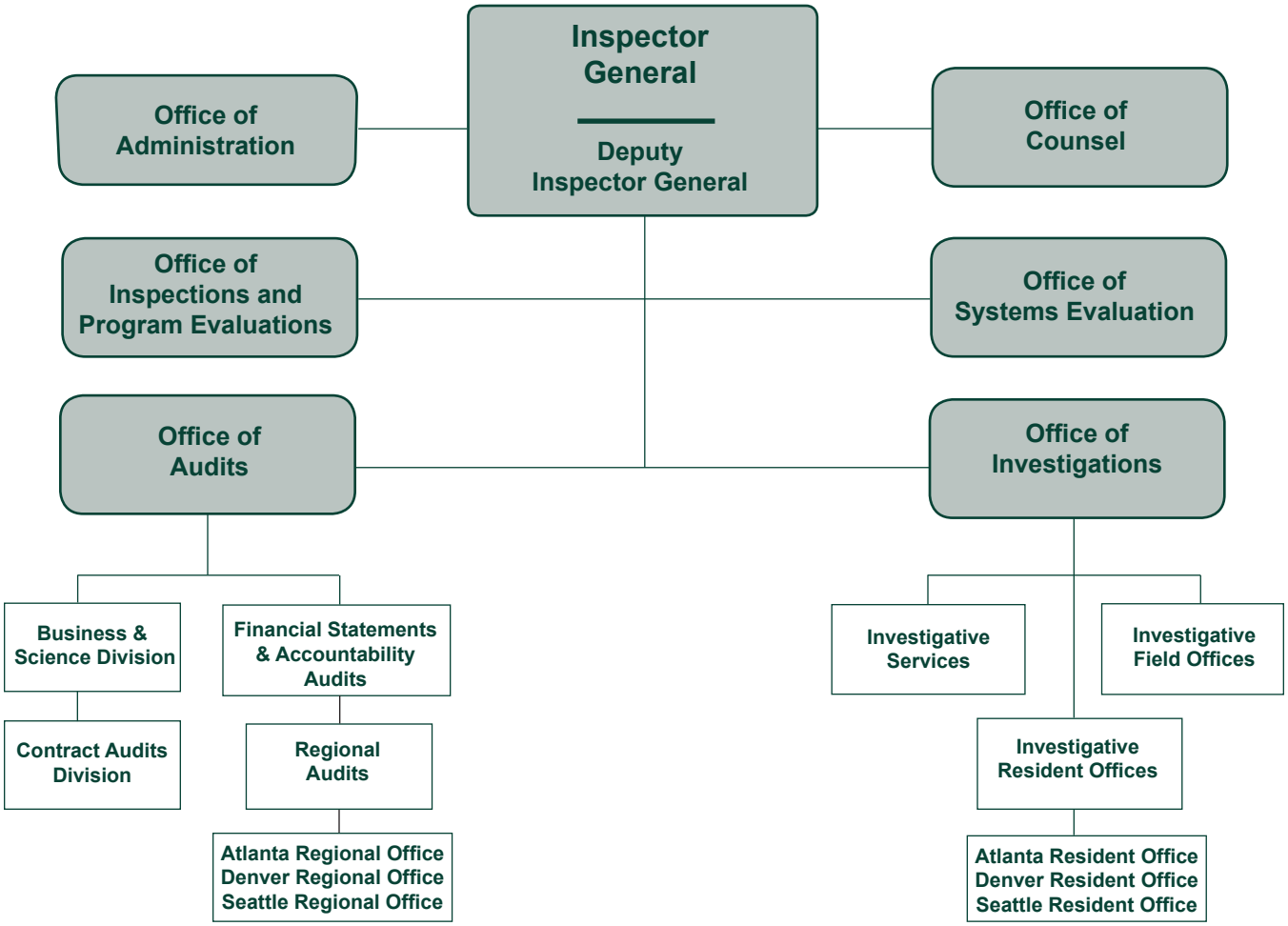
Semiannual Report to Congress

September 2006

OFFICE OF INSPECTOR GENERAL • U.S. DEPARTMENT OF COMMERCE •

Office of Inspector General Organizational Chart



OIG Points of Contact

Inspector General	(202) 482-4661
Legislative and Intergovernmental Affairs	(202) 482-2187
Office of Audits	(202) 482-1934
Office of Administration	(202) 482-2637
Office of Counsel	(202) 482-5992
Office of Inspections and Program Eval.	(202) 482-2754
Office of Investigations	(202) 482-0934
Office of Systems Evaluation	(202) 482-6186
Media Inquiries	(202) 482-4661

REQUESTS FOR REPORTS:

Telephone ..... (202) 482-1243
Internet e-mail ..... oigweb@oig.doc.gov

OIG HOTLINE:

Telephone ..... (202) 482-2495
or (800) 424-5197
TDD ..... (202) 482-5923
Internet e-mail ..... hotline@oig.doc.gov

OIG Internet Home Page

www.oig.doc.gov

IG's Semiannual Report to Congress

September 2006

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

September 2006

The Honorable Carlos M. Gutierrez
Secretary of Commerce
Washington, D.C. 20230

Dear Mr. Secretary:

I am writing to submit to you, in accordance with the Inspector General Act of 1978, this semiannual report outlining the work and activities of the Office of Inspector General for the 6-month period April 1, 2006, through September 30, 2006. The act requires that we prepare this report twice each year to summarize our assessments of Commerce operations and that you transmit it, with any comments you may wish to add, to Congress within 30 days of receiving it.

This report highlights a number of key issues that continue to warrant management's attention, among them, security of information technology resources. In addition, it includes our recent work in the important areas of the Census Bureau's preparations for the 2010 decennial and management of the environmental satellites program by the National Oceanic and Atmospheric Administration. Both are major initiatives with substantial price tags and large numbers of people involved, and they will surely benefit from close management oversight to correct any problems already in existence and prevent new ones from occurring. Finally, I hope you will take special note of the outstanding investigative work this office has done in this semiannual period.

It is also important to note that Commerce has made substantial progress in addressing some of the top management challenges in recent years. We will continue to work closely with you and other senior Commerce managers to ensure that Department resources are always used effectively and efficiently.

It is a pleasure to work with you and your management team, and I extend my personal thanks for partnering with us in a spirit of cooperation.

Sincerely,

Johnnie E. Frazier

CONTENTS

IG's Message to Congress 1

Major Challenges for the Department 3

Strengthen Department-Wide Information Security 3
Effectively Manage Departmental and Bureau Acquisition Processes 6
Strengthen Internal Controls over Financial, Programmatic, and Business Processes 6
Ensure that USPTO Uses Its Authorities and Flexibilities as a Performance-Based Organization to Achieve Better Results 7
Control the Cost and Improve the Accuracy of the Decennial Census 7
Effectively Manage the Development and Acquisition of Environmental Satellites 9
Promote Fair Competition in International Trade 10
Effectively Manage NOAA's Stewardship of Ocean and Living Marine Resources 11
Aggressively Monitor Emergency Preparedness, Safety, and Security Responsibilities 11
Enhance Export Controls for Dual-Use Commodities 12

Agency Overviews

Economic Development Administration 15
Economics and Statistics Administration 21
International Trade Administration 25
National Oceanic and Atmospheric Administration 29
Technology Administration 39
Department-Wide Management 43

Office of Inspector General 47

Office of Investigations 47
Other OIG Activities 50
Tables and Statistics 53
Reporting Requirements 62

Types of OIG Work Products 64

IG's Message to Congress

I am proud to send you this compilation of the work our office has completed during the second semiannual period of fiscal year 2006. My staff continues to perform audits, inspections, and other work that result in significant returns to the American people, either in actual dollars returned to the U.S. Treasury or through far-reaching systemic improvements in programs and operations that yield better delivery of services to American taxpayers and increased efficiency and accountability. Our investigators also have continued their outstanding work, having, for example, pursued and won a conviction with long prison time for a former National Oceanic and Atmospheric Administration employee who had used government computer resources to view child pornography.

Prevention is the underlying reason for much of what we do and what the IG Act expects us to do. It is the reason we spend so much staff time working with recipients of Commerce grants to make sure they understand the importance of using the funds properly. And prevention is the reason we hold many one-on-one and, often, informal—but most effective—meetings with Commerce managers and stakeholders, who understand very well the old saying, "An ounce of prevention is worth a pound of cure."

Although the Department of Commerce has made great strides in improving an array of critical activities during these past months—as evidenced by our removal of one issue from the list of top management challenges earlier this year—we have identified issues that require sustained management attention and close oversight. Clearly, there can be no doubt that the NOAA's triagency environmental satellite program is an example of management weakness, as shown by testimony before Congress in May 2006. Our audit showed the program suffered systemic problems that led to soaring overruns of the project's costs.

NPOESS Program Failings

The National Polar-orbiting Operational Environmental Satellite System (NPOESS) is intended to replace the current generation of civilian and military weather satellites as they reach the end of their useful lives. Largely as a result of problems with a critical sensor, by September 2005 NPOESS was $3 billion over budget and well behind schedule. Yet, the contractor had received more than $123 million in award fees. We uncovered two overarching management and contract weaknesses that contributed to the unchecked cost and schedule overruns.

First, we found that while the sensor problems were communicated to the program's executive committee (EXCOM), the EXCOM did not effectively challenge the integrated program office's optimistic assessment of their impact. Though it was clear by December 2002 that both costs and delays were increasing, the program director—a NOAA employee—maintained that these problems would be solved within available funding reserves and that NPOESS remained on schedule, and his assessment was never effectively challenged. Three years later it was clear the first satellite launch was going to be delayed, but it was too late to turn the program around.

Second, the NPOESS experience shows that the incentive structure used to reward contractors does not always result in top performance as intended. Despite ongoing, significant delays and cost overruns, we found the prime contractor was awarded nearly the maximum fee amounts for the first five billing periods. These payments were the result of a flawed award fee plan which, among other things, contained evaluation criteria that did not sufficiently tie award fees to completion of the most critical or high-risk tasks.

Since our report was released, the Deputy Secretary of Commerce has stressed the importance of NPOESS to the Department's mission and national responsibilities and noted that he now receives

monthly NPOESS progress reports from NOAA. He is working with the Under Secretary for Oceans and Atmosphere and the EXCOM partners to ensure NPOESS is managed, operated, and monitored in a way that meets the intent of our recommendations as well as those of the Nunn-McCurdy review process of the FY 1982 National Defense Authorization Act, which determined that the program should continue with a reduced number of satellites with scaled-back capabilities.

NOAA and Department officials have provided a detailed action plan to address the management and contract weaknesses we identified. We also have identified the development and acquisition of environmental satellites as a top management challenge for the Department and plan to monitor both NPOESS and the Geostationary Operational Environmental Satellite (GOES) program for as long as necessary to ensure the billions spent provide value to the government and the nation.

Prevention Is the Foundation of Our Work

Prevention is the lynchpin of my philosophy as Commerce's Inspector General. A sustained effort to prevent problems whenever opportunity presents itself, to nip in the bud the worrisome things that could become major resource drains, and to offer wise counsel when a program seems to work but is hampered by strings of small inefficiencies that add up to overall ineffectiveness all characterize the outstanding work our office has consistently performed.

Prevention is the underlying reason for much of what we do and what the IG Act expects us to do. It is the reason we spend so much staff time working with recipients of Commerce grants to make sure they understand the importance of using the funds properly. And prevention is the reason we hold many one-on-one and, often, informal—but most effective—meetings with Commerce managers and stakeholders, who understand very well the old saying, "An ounce of prevention is worth a pound of cure."

Prevention by Deterrence

Prevention also serves as the motivation for our dedicated investigators who have to dig deep into the uglier side of human activity on occasion in the hope that shutting down one bad guy would serve as a warning to any others who might be tempted to betray the trust of their government position. It is not with pleasure, but a grim satisfaction, that I must note that Commerce OIG investigators' dogged pursuit of one case drew national media attention and ended with the unsavory perpetrator being sentenced to many years in prison.

On May 19, 2006, a former NOAA employee entered a guilty plea to federal charges of possession and production of child pornography. The man admitted to using government computers to download child pornography for approximately 10 years at work. The investigation, which was conducted by forensic experts in our Computer Crimes Unit, revealed more than 1 million pornographic images of children on his home and office computers. A search of his residence also uncovered evidence that he also was involved in the production of child pornography.

The suspect fled the United States after his December 21, 2005, indictment and was featured on the television show *America's Most Wanted* in January 2006. A few days after the program aired, he turned himself in to U.S. officials in Rome, Italy. He was sentenced on August 30, 2006, to 15 years in prison, followed by 3 years of supervised release, and ordered to pay restitution to a victim identified during our investigation.

This disturbing case is now complete and the perpetrator incarcerated. But we are challenged to find ways to prevent such things, as well as go after any new instances of wrongdoing as they come to light.

Collaboration Is Key to Future Success

And finally, I am encouraged by the active role Secretary Gutierrez and Deputy Secretary Sampson have taken to improve the overall management of the Department. Not only have they promulgated a set of priority issues requiring the Department's sustained attention, several of which complement our list of management challenges, they also have stressed their desire that their management team should actively collaborate with us to address areas of mutual concern.

I look forward to deepening our working relationship with Secretary Gutierrez, Deputy Secretary Sampson, Congress, and senior Department officials as we take on the important challenges facing Commerce. Meeting the goals of the Inspector General Act requires that we act only in sincere partnership to provide the American people the highest quality and highest functioning government possible. Working together, I am confident that we can achieve that goal.

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. Each challenge meets one or more of the following criteria: (1) it is important to the Department's mission or the nation's well-being, (2) it is complex, (3) it involves sizable resources or expenditures, or (4) it requires significant management improvements. Because of the diverse nature of Commerce activities, these criteria sometimes cut across bureau and program lines. Experience has shown that by aggressively 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 Department-wide information security.
2. Effectively manage departmental and bureau acquisition processes.
3. Strengthen internal controls over financial, programmatic, and business processes.
4. Ensure that USPTO uses its authorities and flexibilities as a performance-based organization to achieve better results.
5. Control the cost and improve the accuracy of the decennial census.
6. Effectively manage the development and acquisition of environmental satellites.
7. Promote fair competition in international trade.
8. Effectively manage NOAA's ocean and living marine resources stewardship.
9. Aggressively monitor emergency preparedness, safety, and security responsibilities.
10. Enhance export controls for dual-use commodities.

Challenge 1

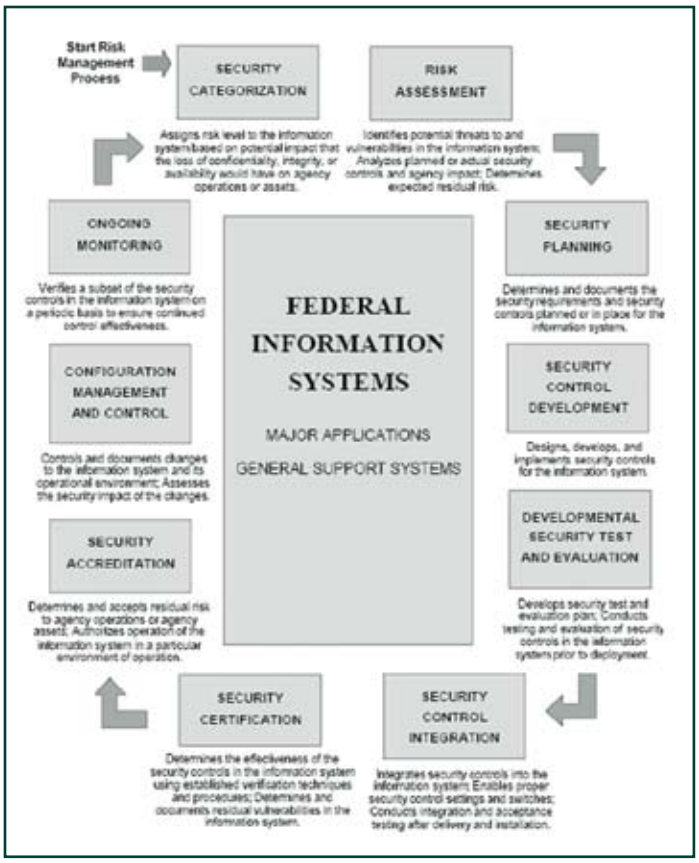
Strengthen Department-Wide Information Security

Since enactment of the Federal Information Security Management Act (FISMA), government agencies have devoted significant resources to improving the security of information stored on their computer systems. The problem is long standing: GAO has identified information security as a government-wide high-risk issue every year since 1997. At Commerce, it is the No. 1 challenge and has been a material weakness since 2001.

To eliminate the material weakness, Commerce has emphasized improving its certification and accreditation (C&A) process for IT systems. In February 2005, the chief information officer (CIO) issued a plan to produce acceptable quality C&A packages for all national-critical systems and some mission-critical systems by the end of FY 2005 and for all other systems by the end of FY 2006. In light of that plan, our approach to the C&A portion of our 2005 FISMA evaluation was to review all improved packages available by August 31, 2005. Only five were ready—three from NOAA and two from Census. Those packages showed some noteworthy improvements. However, with such a low number of packages available for review and considering the deficiencies we found, we concluded that the Department's C&A process had not improved to the point where authorizing officials had sufficient details about remaining system vulnerabilities to make fully informed accreditation decisions, and the IT security material weakness remained.

In early FY 2006, the acting CIO worked with the operating units to reassess the schedule and give units more latitude on time frames for completing improved C&A packages, which recognized that the amount of time necessary to complete the C&A process correctly had been continually underestimated. When revised schedules were finalized in June 2006, the Department's Office of the CIO (OCIO) expected a total of 28 C&A packages to be completed by the end of July, 27 of which were for high- or moderate- impact systems.[1] OCIO reviewed completed packages and worked with the bureaus to address concerns, as necessary. If OCIO determined a package was of sufficient quality, it was forwarded to OIG for FISMA review. As of August 24, 2006, our agreed-upon cutoff date, the CIO's office had received packages for 22 high- and moderate-impact systems, 12 of which were forwarded to us. We evaluated a total of 15 C&A packages for FY 2006 FISMA reporting. Eleven of these packages were Commerce-owned systems that had gone through the improvement process, and 4 were high- and moderate

[1] Commerce systems were previously categorized as national critical, mission critical, or business essential. With the publication of NIST Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, agencies must now categorize information and information systems as low, moderate, or high impact, based on the potential consequences to organizations and individuals should there be a breach of security.



Source: http://csrc.nist.gov/policies/WhatAgencycandonow-OMB-memo.pdf

impact contractor systems that had not. (FISMA requires OIGs to review contractor systems.)

We found a larger percentage of C&A packages met the requirements of Commerce's IT security policy and applicable National Institute of Standards and Technology (NIST) standards and guidance (33 percent) as compared to last year (13 percent). But progress has been slow. Overall, we found that security plans and risk assessments have continued to improve. Security plans have shown particular improvement in the identification of network components. To be consistent with NIST standards and guidance and better support selection and tailoring of security controls, risk assessments now need to focus on specific threats and vulnerabilities for a given system instead of considering all possible risks.

We also found significant improvement in testing of the five systems we reported as certified and accredited, as well as in testing of a system granted interim authorization to operate. However, the remaining nine systems had serious deficiencies in the assessment of security controls, particularly in the testing of operational and technical controls needed to determine whether the security controls for network components are in place and operating as intended. That being the case, neither the certification agent nor the authorizing official had adequate information on the remaining vulnerabilities, and we again found this to be a material weakness within Commerce.

Our review included two draft C&A packages for USPTO contractor systems, which we found to be of poor quality. Therefore, we also recommended that USPTO, which submits its performance and accountability report separately, report IT security as a material weakness.

Protection of Sensitive Agency Information

After a recent series of incidents throughout the federal government involving the compromise or loss of sensitive personal information, the Office of Management and Budget (OMB) issued Memorandum M-06-16 on June 23, 2006. The memorandum emphasized the need to protect personally identifiable information that is remotely accessed or physically removed from an agency location, required agencies to ensure that appropriate safeguards were in place within 45 days, and asked inspectors general to conduct reviews.

OMB defines personally identifiable information as "any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual."[2]

OMB's memorandum included a checklist prepared by NIST for protection of remote information and recommended four additional actions: (1) encrypting all sensitive agency data on mobile computers/devices, (2) allowing remote access only with two-factor authentication,[3] (3) using a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity, and (4) logging all computer-readable data extracts from databases holding sensitive information and verifying such extracts have been erased within 90 days if no longer needed.

The President's Council on Integrity and Efficiency (PCIE) prepared a review guide for inspectors general and was to provide a government-wide report to OMB in October based on input from IG reviews of their agencies.[4] To evaluate Commerce, we selected a sample of 10 systems. This represents 16 percent of all systems identified by Commerce bureaus as storing or processing person-

[2] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 14, 2006.

[3] Two-factor authentication is achieved by authenticating two of the following three factors: 1) "something you know" (e.g. a password), 2) "something you have" (i.e. in your possession at the time of the authentication), or 3) "something you are" (e.g., a biometric such as your fingerprint)

[4] The PCIE was established by Executive Order 12805, May 11, 1992, to address integrity, economy, and effectiveness issues that transcend individual government agencies, and increase the professionalism and effectiveness of IG personnel throughout the government.

ally identifiable information and accessed remotely or physically removed from an agency location. We reviewed the current system security plan and all test results verifying that the applicable controls are in place for each of these systems.

Because of the short time available to perform our work (results were due to PCIE on September 22), our review was limited in scope, relying primarily on a comprehensive examination of security control test results provided by the operating units. Our FISMA work plan for FY 2007 includes actual testing of applicable security controls.

We found that in most cases bureaus could not demonstrate that the necessary steps have been taken to ensure that personally identifiable information is adequately safeguarded. None of the system documentation reviewed indicated that personally identifiable information was stored or processed, a step needed to determine the required safeguards. The Department's IT security policy does not explicitly address the protection needs associated with personally identifiable information that is accessed remotely or physically removed. The Department's OCIO has indicated that a revised policy addressing personally identifiable information requirements will be available during FY 2007. Most of the systems we reviewed showed no evidence that required protections for personally identifiable information transported and stored offsite, such as encryption, are implemented. There also was no evidence that protections are in place for remote access of personally identifiable information, such as virtual private networks or controls on downloading and storage of such data.

To address the loss of sensitive personal information from laptop computers and related equipment at the Census Bureau, the Secretary of Commerce asked OIG to determine the extent of problems in protecting sensitive personal information at Census, including whether property management policies and practices are adequate in light of the bureau's unique workforce and mission. We plan to report on the results of our evaluation in the next semiannual.

NOAA C&A

In this semiannual period, we reported on findings from our FY 2005 review of three NOAA C&A packages: the Search and Rescue Satellite-Aided Tracking system (SARSAT), the Polar Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified by NOAA personnel and accredited by a senior NOAA official as part of NOAA's C&A improvement effort.

Our report focused on two problem areas: incomplete system descriptions and inadequate security control assessments. Insufficiently complete system descriptions can yield inadequate identification and examination of system components in security control assessments. The security control assessments did not evaluate many of the system controls and were conducted without adequate test procedures. Consequently, NOAA's certification process did not provide sufficient information to authorizing officials on remaining system vulnerabilities.

In its response, NOAA stated that it had completed C&A activities for POES and SARSAT nearly 14 months ago, had made immediate changes to its C&A process after our December 2005 exit conference, and has implemented most of the changes recommended in our report. However, as we noted in our report, we prepared the report because some of the problems we identified in our FY 2005 and previous reviews were still evident in the additional five NOAA C&A packages we reviewed early in FY 2006. We hope that documenting our concerns in this report and making formal recommendations for improvement will facilitate complete correction of these issues, many of which have persisted for some time. (See page 33.)

NOAA E-Authentication

E-authentication is the process of electronically verifying the identities of users accessing government services over the Internet and is crucial to the Department's ability to properly authorize access to data and hold users accountable for their actions. We evaluated the quality of NOAA's e-authentication risk assessment and controls for SARSAT—the U.S. portion of an international program that uses satellites to coordinate search and rescue activities. These controls, implemented for two SARSAT web-based applications, provide a first line of defense for beacon registration data that is protected under the Privacy Act. According to NOAA's e-authentication risk assessment, one consequence of unauthorized use of the SARSAT beacon registration system is that search and rescue personnel could waste valuable time using incorrect or misleading data.

The objectives of our review were to determine if the risk assessment adequately identified the requirements for e-authentication controls and whether the controls had been implemented and properly certified prior to the system's accreditation. Our evaluation found that SARSAT's e-authentication controls do not provide adequate assurance of users' identities and recommended that NOAA redo the e-authentication risk assessment to better characterize and assess authentication risk, improve the system security plan to identify e-authentication requirements and appropriate controls, test controls, and take actions to correct deficiencies.

NOAA disagreed with our conclusion that SARSAT's e-authentication controls do not provide adequate assurance of users' identities, but agreed with all but one of our recommendations. After we clarified the meaning of that recommendation—to document any deficiencies identified as a result of performing e-authentication control testing—NOAA agreed with it as well. (See page 31.)

IT Security Clauses in Contracts

We conducted an evaluation to determine whether NOAA is incorporating the two information security clauses prescribed by the Department into contracts and to evaluate implementation of the clause requirements. Clause 73 requires contractors to comply with the Department's IT security policy and have their IT resources certified and accredited if they connect to a Commerce network or process or store government information. Clause 74 requires contractor personnel to undergo appropriate background screening and IT security awareness training.

We reviewed a judgmental sample of 16 NOAA service contracts and interviewed managers and staff from NOAA's Office of Acquisition and Grants, Office of the Chief Information Officer, and line offices. Because some problematic aspects of Clause 73 contributed to issues we identified at NOAA and in a previous review at USPTO, we also made recommendations to Departmental officials. Our report highlighted the need to clarify the requirement to include Clause 73 in all contracts in which contractor IT resources are either connected to a government trusted network or are allowed privileged access to government information. For the Department, the evaluation identified needed improvements to the IT security clause and the *Commerce Acquisition Manual* as well as the need for developing additional guidance to aid contracting officers and contracting officer representatives in their oversight of contractor information security. For NOAA we identified improvements needed for ensuring the certification and accreditation, as appropriate, of contractor IT resources.

Both the Department and NOAA agreed with our recommendations. On September 27, 2006, in response to our recommendations, the Department's director of acquisition management and procurement executive issued a procurement memorandum and *Commerce Acquisition Manual* notice with revisions to the clause and changes to the approach to determine the level of contract risk so that personnel receive background investigations commensurate with the risk level. (See page 35.)

Challenge 2

Effectively Manage Departmental and Bureau Acquisition Processes

Commerce spends nearly $2 billion annually on goods and services—roughly a third of its annual appropriation—and each year relies more on contractors to support its mission-critical work. Adequate oversight of acquisition planning and execution is essential to ensuring that taxpayers dollars are spent effectively and efficiently and procurement laws and regulations are followed.

For example, the Census Bureau's contracting for products and services to support 2010 decennial operations continues to bear watching. The bureau estimates that 17 percent ($1.9 billion) of its 2010 budget will be spent on contracts for information technology systems, advertising, and leases for local office space. One key IT program—Field Data Collection Automation (FDCA)—will develop the handheld mobile computers that field staff will use to collect 2010 decennial information. This is a critical piece of the bureau's reengineered strategy. Census originally planned to develop this equipment in-house but determined in early 2004 that it lacked the management and technical resources to do so, and on March 31, 2006, awarded a system development contract. However, the late decision to use a contractor and the initial slow pace in planning the acquisition shortened the amount of time available for awarding the contract and developing FDCA. This will delay address canvassing, the first major field operation of the dress rehearsal for the 2010 census.

Challenge 3

Strengthen Internal Controls Over Financial, Programmatic, and Business Processes

Internal controls are the steps agencies take to make sure their operations are effective, efficient, and in compliance with laws and regulations. Internal controls also ensure that financial reporting is reliable, and assets are safeguarded from waste, loss, or misappropriation, according to the Office of Management and Budget (OMB). Two documents, the Federal Managers' Financial Integrity Act (FMFIA) and the 2004 revision of OMB Circular A-123 (Management's Responsibility for Internal Control), set out internal control requirements for the federal government: Commerce and all federal agencies must define and document major financial internal control processes and test key financial controls to determine whether they are effective as of June 30, 2006.

Although we noted recent improvement in the Department's management and financial accountability as well as in program and operational effectiveness, our audits continually indicate more work is needed to strengthen internal controls over programs, operations, and administrative areas.

We expect the new federal emphasis on strong internal controls to create a number of new demands for OIG reviews in the coming years. For example, the Digital Television Transition and Public Safety Act of 2005 puts NTIA, one of the Department's smaller agencies, in a position of having to manage an enormous national project with an even larger budget than had been anticipated. Successfully implementing this act will constitute a significant management challenge for the Department. We will share lessons learned

from our work in other areas to help the agency design strong, well-structured programs and minimize opportunities for fraud.

Challenge 4

Ensure that USPTO Uses Its Authorities and Flexibilities as a Performance-Based Organization to Achieve Better Results

Since March 2000 when the Patent and Trademark Office Efficiency Act transformed USPTO into a performance-based organization designed to operate more like a private corporation than a government agency, OIG has paid close attention to a number of aspects of the organization's internal management structures and practices.

USPTO faces numerous challenges, such as a continuing increase in applications, training about 1,000 newly hired examiners in Patents and Trademarks, and transitioning to an electronic processing environment. In addition, USPTO's expanded authority over personnel decisions and processes, procurement, and information technology operations needs to be effectively and efficiently utilized.

OIG has issued nearly a dozen reports examining problems at USPTO since 2001. The bureau has generally taken decisive action to address some problems we identified in the past, and we have been pleased that USPTO has been receptive to our recommendations. But ultimately, we believe that many of the problems USPTO suffers are serious and require the sustained commitment of senior managers to resolve. OIG will continue to monitor the bureau's progress.

A USPTO trademark information specialist assists customers.

Source: USPTO

Challenge 5

Control the Cost and Improve the Accuracy of the Decennial Census

Even after adjusting for inflation, the 2010 census will be the country's most expensive decennial ever—estimated to cost $11.3 billion. The Census Bureau's redesigned decennial plan, established after the 2000 Census, is heavily dependent on automating critical field operations to accurately count the nation's population within budget. The bureau has established a rigorous testing schedule to monitor development and implementation of the strategy, identify problems, and incorporate solutions in time for the decennial.

During the last 6 months, we built on the work we did in 2005 and early 2006, which reviewed the 2006 test's address canvassing operation. This semiannual report details our review of Census's test to enumerate the group quarters population (see page 21).

Although most U.S. residents live in residential housing units such as single-family houses, apartments, and mobile homes, more than 7 million people live in situations such as college dormitories, nursing homes, prisons, and group homes, collectively known as group quarters. We reviewed the group quarters testing operation at the Census Bureau's test site in Travis County, Texas. The area is ideal for testing the group quarters operation because it is home to four universities and colleges, a state prison, and numerous other group living facilities.

New Methods, New Challenges

Our review found that although the bureau is working on new methods to better enumerate the group quarters population, it continues to face a number of challenges. For example, nontraditional student housing, such as private dorms and student cooperative housing, did not easily fit into any of Census's group quarters definitions. Sometimes these units were defined as private residences and received housing unit questionnaires. In those cases, there was an increased likelihood that the unresponsive students had already moved out of their residence before the follow-up operation. When this occurred, enumerators relied on records kept in administrative offices, which often lacked Hispanic origin and race information. We also found that 42 percent of the validation workload was associated with large apartment complexes erroneously identified as potential group quarters during address canvassing. This caused problems in the group quarters validation and the nonresponse follow-up operations.

One of the objectives of our review was to independently assess the completeness of the group quarters listing prepared for the Census 2006 test. The bureau used four sources to develop a list of all potential group quarters for the 2006 test, which was then

Group Quarters Activities in the 2006 Census Test				
Operation	**Group Quarters List Development**	**Address Canvassing**	**Group Quarters Validation/Advance Visit**	**Group Quarters Enumeration**
Dates	June 2004—with updates throughout 2006 Census Test	July 2005—September 2005	December 2005—January 2006	April 2006—May 2006
Description	List created using • 2000 group quarters • Administrative records • Address canvassing (Other Living Quarters) • Other Census survey work	Identified potential "Other Living Quarters" (OLQs) Ensured addresses were correct and/or made changes to update the Master Address File	Listers visited 1,778 OLQs in Austin and 84 OLQs on the Cheyenne River Reservation to designate address status as a • GQ • Housing Unit • Nonresidential • Vacant • Transient • Duplicate • Other Group quarters administrators contacted regarding upcoming group quarters enumeration; privacy and confidentiality were discussed	Enumeration of all identified group quarters facilities

Source: U.S. Census Bureau, *2006 Census Test Project Management Plan,* 2010 Census Memoranda Series No. 8 (Reissue) December 2005

refined by the group quarters validation operation, resulting in a final list of group quarters to be enumerated. We found a number of group quarters that were not on the final enumeration list by conducting a limited Internet search and speaking with administrators. We also found duplicates—addresses that appeared on both the enumeration and housing unit lists or group quarters that appeared twice on the enumeration list. These errors can result in an inaccurate count of the population because individuals living in group quarters enumerated via the household questionnaire may be missed and duplicates on the list can result in people being counted twice.

We also found that Census should take additional steps to count the student population, such as working closely with fraternity and sorority campus oversight organizations and exploring the use of the Internet as a response option for this computer-oriented generation. Finally, we noted that some additional group quarters processes and procedures warrant management attention.

More than a dozen group quarters—and possibly many more—were not on the Census Bureau's enumeration list. This home is one of 15 missing from the list that we found by conducting a limited Internet search.

Source: OIG

Looking Ahead

We continue to look at the update/enumerate operation at the Cheyenne River Reservation and Off-Reservation Trust Land in South Dakota. During this operation, which is used in communities where residents are less likely to return a completed questionnaire,

enumerators update the address lists and maps and interview a resident to complete a questionnaire for each housing unit. We are assessing whether the update/enumerate operation obtained complete and accurate enumerations, especially with respect to large households, and if it resulted in improved address lists and maps. We are also assessing the bureau's method for designating which communities require this type of enumeration.

Challenge 6

Effectively Manage the Development and Acquisition of Environmental Satellites

Over the next 5 years, the Department, through NOAA, will spend several billion dollars in contracts for the purchase, construction, and modernization of environmental satellites.[5] These systems, operated by NOAA's National Environmental Satellite, Data and Information Service (NESDIS), collect data to provide short- and long-range weather forecasts and a variety of other critical environmental and climate information.

Complex, high-cost acquisitions such as these are extremely difficult to manage within cost and schedule goals, as was revealed in our audit during this reporting period of the National Polar-orbiting Operational Environmental Satellite System (NPOESS) (see page 29). This system—a joint project of NOAA, NASA, and Defense—is critical to the nation's ability to provide continuous weather and environmental data for civilian and military needs through the coming 2 decades. Initially projected to cost $6.5 billion, the program recently underwent a mandatory congressional review to see if it should be continued, given its troubling history of huge cost increases and schedule delays.

Congress Approves a Scaled-Back NPOESS Program

Last November, the Department of Defense reported that NPOESS costs had grown by 25 percent over original estimates—triggering the Nunn-McCurdy recertification provision of the FY 1982 National Defense Authorization Act. In addition to these staggering cost increases, the program was running 17 months behind schedule yet the contractor had received $123 million in incentive payments.

We sought to determine how cost and schedule overruns had grown so dramatically while the contractor had been so well rewarded. We identified serious shortcomings in the contract's incentive structure as well as in program oversight from NPOESS' executive committee, which consists of top leadership from NOAA, NASA, and Defense.

Source: http://goes.gsfc.nasa.gov/images/GOES-R_Color_Lg.jpg

Commerce IG Johnnie E. Frazier reported our findings to the House Science Committee in May (see page 50), as the recertification process was in progress. In June, the Committee accepted a triagency proposal to continue the program with the following changes:[6]

- Total acquisition costs were revised to $11.5 billion to support NPOESS satellite coverage through 2026.
- The number of satellites was reduced from six to four, with the U.S. relying on European satellites to fill in any gaps resulting from the reduction.
- The first satellite will launch in 2013 rather than 2010, as proposed in the original program.
- The number of sensors will drop from seven to five.
- Management reforms, including our recommendations for improving EXCOM oversight and revising the award fee contract, will be implemented.

This program will continue to bear close watching as it restructures and attempts to stay within its new cost and schedule goals, and we intend to follow its progress and keep Congress apprised of our findings.

GOES-R Costs, Schedule, and Capabilities Are Being Redefined

The GOES-R series is the next generation of geostationary satellites that will replace existing GOES satellites in the next decade. The new series will have enhanced sensing capabilities that are expected to offer an uninterrupted flow of high-quality data to support weather forecasting, severe storm detection, and climate research vital to public safety. GOES-R is a multicontract, mul-

[5] http://www.osec.doc.gov/bmi/Budget/05APPR/PAR05.pdf, page 210
[6] http://www.house.gov/science/hearings/full06/June%208/charter.pdf

tiyear program wholly funded by Commerce, though the new satellites will be developed and acquired with help from NASA. The Department's investment for GOES-R for fiscal years 2006 to 2010 is projected at about $2 billion.

Planning for the new series, which has been under way for the past 5 years, has given long and careful focus to the many risks inherent in developing satellite programs. Even so, the NPOESS experience has put new pressure on agency senior officials and program planners to have strong mechanisms in place for tracking every phase of the program and promptly mitigating problems that arise.

During this semiannual period, we initiated a joint review of the GOES-R program with NASA's Office of Inspector General. Our shared objective is to determine whether the Department and NASA have created a management structure to ensure effective oversight of the many risks associated with the GOES-R program. In preparing for the review, we learned that the Department, NOAA, and NASA are restructuring major aspects of the program as part of detailed risk reduction activities. GOES-R leadership is reassessing planned satellite capabilities and the timing of launches in response to input on costs and technological risks provided by an independent review team and contractors involved in defining the program's major aspects. In addition, program officials are considering changing approaches to managing the program and acquiring the satellites.

At Commerce, the oversight component of our work will look at the Department and NOAA's efforts to establish effective monitoring organizations, policies, and procedures and the mechanisms NOAA will use to leverage NASA's oversight expertise. We will also consider whether program staff report significant issues to senior Department and NOAA oversight officials in a timely fashion and whether those officials take appropriate action.

Our acquisition focus will be on the program office's overall approach to procuring key satellite instruments, identifying potential risks, and implementing associated mitigation strategies. We will also assess the acquisition contracts' award fee plans to determine whether they are structured to promote excellent performance.

NASA OIG plans to determine whether NASA program management councils effectively identify and review program issues and progress, and whether procedures and processes are in place to recognize, mitigate, and report technical risks in accordance with NASA policy.

Challenge 7

Promote Fair Competition in International Trade

The Department of Commerce accomplishes its goals of promoting trade, opening overseas markets to American firms, and protecting U.S. industry from unfair competition by imports primarily through the work of the International Trade Administration (ITA). ITA also works with USPTO and NIST to assist U.S. companies with intellectual property rights and standards. Over the past several years, OIG has focused a number of reviews on the Department's

Source: U.S. Census Bureau

efforts to increase U.S. market opportunities, provide assistance to U.S. exporters, and overcome trade barriers in difficult foreign markets.

In September 2006, in response to OIG recommendations made to ITA in several recent reports, the bureau's Commercial Service (CS) announced extensive changes in its procedures for verifying export success claims, its primary performance measure. CS stated that the new procedures were necessary because, in a significant number of cases, OIG had found discrepancies in the reported export successes. These discrepancies raised doubts about the integrity of the data CS reports to Congress and the administration on its accomplishments. The new CS procedures require improved documentation, supervisory confirmation of a sample of export success reports, and verification that CS provided value-added assistance.

In response to a request from the House Small Business Committee, we are reviewing coordination and information sharing between Commerce and other U.S. government agencies with responsibility for trade promotion. The review, which we will discuss in our next semiannual report, will assess Commerce's efforts to match export opportunities with export-ready companies, with a focus on trade promotion agencies' use of the Internet to communicate leads and other relevant trade information.

U.S. Trade Promotion in South America

During this semiannual period, we conducted on-site inspections of CS posts in Brazil, Argentina, and Uruguay. Significant export opportunities are opening in these countries as Brazil's large economy continues its steady growth, Argentina recovers from its 2001-2002 economic crisis, and Uruguay pursues closer trade relations with the United States. Our inspections focused on the management, program operations, and financial and administrative practices of these three South American posts. We issued our report on CS' operations in Argentina and Uruguay in September with 20 recommendations, and we will publish our report on CS' larger post in Brazil before the end of the calendar year.

Our review of CS Argentina and CS Uruguay found that the posts are providing useful export assistance to U.S. companies and have established collaborative relationships with key U.S. government offices and nongovernmental organizations both in those countries and in the United States. Our review found effective administrative management practices at both posts, but we also identified some financial management and accounting concerns that warrant the attention of Commerce managers (see page 25).

Challenge 8

Effectively Manage NOAA'S Stewardship of Ocean and Living Marine Resources

The National Oceanic and Atmospheric Administration is charged with monitoring the health of our nation's ocean, coastal, and Great Lakes resources; administering civilian ocean programs; and protecting and preserving the nation's living marine resources through scientific research, fisheries management, enforcement, and habitat conservation.

During the past year, we followed up on our audit of the National Marine Fisheries Service's (NMFS') preparation of a biological opinion for California's Central Valley Project, one of the nation's major water conservation efforts. In response to our audit recommendations, NOAA received three reviews of the opinion. One review concluded that NMFS used the best scientific information for the biological opinion, but two reviews concluded that NMFS did not. In light of these findings, we asked NOAA officials to submit to us a plan that identifies actions they will take to address the deficiencies and implement the related recommendations made by the independent review organizations.

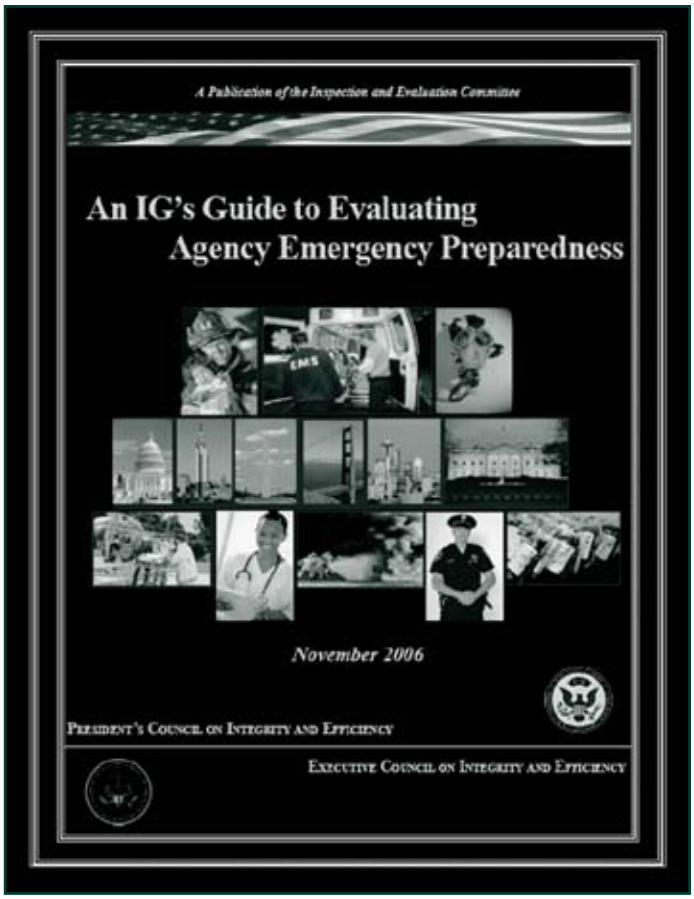
NOAA's future challenges include its efforts as a steward of marine resources, the agency's consultation process, and its management of fisheries and marine mammals.

Challenge 9

Aggressively Monitor Emergency Preparedness, Safety, and Security Responsibilities

The Department of Commerce has a dual responsibility in the area of emergency preparedness, safety, and security; not only must it be ready to protect 35,000+ employees and hundreds of facilities, but because several Commerce programs are critical to national preparedness and recovery efforts, it must support U.S. efforts to prepare for, respond to, and promote recovery from major disasters.

We continue to monitor Commerce's progress in resolving departmental emergency preparedness and security weaknesses we identified in assessments conducted in 2002 and 2005. Although Commerce has made significant improvement in emergency preparedness to address some of the vulnerabilities, we found,



Source: OIG

among other things, the need for better departmental guidance and oversight of emergency programs, risk assessments, occupant emergency plans, and security forces at its domestic operations, as well as better oversight of security upgrades and greater attention to security at its overseas offices.

More recently, in our review of the Commerce workers' compensation program, we recommended that the Department consolidate and analyze bureau safety data to help officials and managers identify and correct problems. We also recommended the Department use this data to find ways to help prevent workplace injuries and lower the number of employees who file claims for workers' compensation benefits.

Finally, we are working with other PCIE members to publish a guide for evaluating emergency preparedness programs. The guide should be a useful tool for conducting future OIG or management reviews of emergency preparedness in Commerce and other federal agencies.

Challenge 10

Enhance Export Controls for Dual-Use Commodities

The Department's Bureau of Industry and Security (BIS) oversees the federal government's export licensing system for dual-use commodities and technology and is charged with advancing U.S. national economic security interests by administering and enforcing export controls. The primary goal of the licensing and enforcement system is to prevent hostile nations and terrorist groups from acquiring sensitive technologies and materials that have both civilian and military applications by controlling their export.

The National Defense Authorization Act (NDAA) for Fiscal Year 2000, as amended, directed the inspectors general of the departments of Commerce, Defense, Energy, and State, in consultation with the directors of Central Intelligence[7] and the FBI, to report to Congress by March 30, 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. (The Office of Inspector General at the Department of Homeland Security also has participated since its establishment in 2003.) In addition, the NDAA for FY 2001 requires the IGs to discuss in their annual interagency report the status or disposition of recommendations made in prior-year reports submitted under the act.

Some Export Control Topics Covered by Interagency OIG Reviews

- Federal automated export licensing systems
- Commerce Control List and U.S. Munitions List
- Deemed exports
- Export enforcement
- Export licensing process for chemical and biological agents
- U.S. dual-use export controls for China
- U.S. dual-use export controls for India (Commerce only)

[7] The Intelligence Reform and Terror Prevention Act of 2004 [Public Law 108-458], dated December 17, 2004, established the Director of National Intelligence to serve as the head of the U.S. intelligence community.

We have initiated our eighth and final NDAA required review, this time looking at the effectiveness of U.S. controls on dual-use exports to India. India presents unique challenges to U.S. commercial interests and export control policy. As one of the fastest growing economies in the world, India offers expanding trade opportunities for U.S. exporters but also increased competition for U.S. industry and labor.

We will detail the findings of our India evaluation in our March 2007 semiannual report. And though this will conclude our statutory reporting requirements under NDAA, we will continue to monitor BIS' efforts to implement and enforce dual-use export controls, given the importance of this mission to the nation's security. We will also follow up on our previous NDAA recommendations and report on BIS' progress in implementing them in our next semiannual report.

These nuclear reactors are among 16 in operation throughout India, and the country has plans to build 6 more over the next 2 years. Under the terms of a July 2006 agreement, the United States will give India greater access to dual-use technology to expand its civilian nuclear program and meet its burgeoning energy needs.

Source: http://as.wn.com/i/d5/8c93997c11de00.jpg and http://www.icjt.org/npp/podrobnosti.php?drzava=11&lokacija=718

ECONOMIC DEVELOPMENT ADMINISTRATION

Chicago Area Nonprofit Managing RLF Grant Poorly

The **Economic Development Administration** was established by the Public Works and Economic Development Act (PWEDA) of 1965 to generate new jobs, help retain existing jobs, and stimulate private investment in economically distressed regions of the United States. EDA continues to fulfill this mission under the authority of PWEDA, as amended by the Economic Development Reauthorization Act of 2004. Based on local and regional comprehensive economic development 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 sudden and 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, planning, training and research, and economic adjustment assistance.

In September 1995, the Economic Development Administration awarded a $500,000 long-term economic deterioration assistance grant to a nonprofit community development corporation in Chicago to remedy actual or threatened economic dislocation in the city and six surrounding suburbs. The grant allocated $450,000 for a revolving loan fund (RLF) and $50,000 for salaries and other expenses. It required $150,000 in matching funds from the recipient.

In August 2001, EDA awarded the organization a second grant for $787,500, allocating $750,000 for the RLF, $37,500 for salaries and expenses, and requiring $787,500 in matching share for similar purposes.

We audited the two grants, which were combined for reporting purposes, for the 10-year period covering September 1995 through December 2005 to assess the financial management of the RLF, verify the allowability of administrative costs, and determine whether the grantee complied with applicable laws and regulations.

What We Found

Our audit disclosed the community development corporation is not managing the RLF effectively. At the end of December 2005, the organization had not met the 75 percent capitalization standard required by EDA regulations and had $419,655 in excess cash. It also had $199,432 in undisbursed grant funds.

The RLF had six active loans with a total outstanding principal balance of $446,251 and funds available for new loans of $708,290. Our audit showed the group had $199,432 of undisbursed grant funds as of December 31, 2005. In the 10-year history of the RLF, the group had made only 12 loans, but it stated in its RLF plan that it expected to make 49 loans in the first 5 years of the RLF. At the time of our audit, the organization had not made an RLF loan since April 2003.

The organization made only one loan ($112,000 EDA portion) within the first 3 years of the financial assistance award, when all $450,000 of EDA loan funding should have been disbursed. The community development corporation's officials said the original award was based on financing manufacturing businesses on the west side of Chicago, which declined precipitously in the mid-to-late 1990s. The surviving firms were averse to taking on more debt. In 2001, the corporation began lending to businesses outside the manufacturing sector, but although it broadened its lending base, it still has a large balance of remaining grant funds.

Unallowable Interest Expense

The group's management said it accrued $142,018 in interest expense from a secondary low-interest loan from the Ford Foundation, which was used to provide part of its required nonfederal matching share. OMB regulations do not allow interest expense to be charged to an RLF.

As of December 31, 2005, EDA award disbursements exceeded EDA's portion of loans made by $29,567. From September 1995 through December 2005, EDA made eight RLF disbursements to the organization totaling $1,000,567. During that period, the group made 12 loans totaling $1,639,000 (including refinancing of some of the loans). The EDA portion of the 12 loans totaled $971,000, and the organization's matching portion of the 12 loans totaled $668,000. According to EDA RLF standard terms and conditions, an RLF grant recipient must request disbursements from EDA only at the time and in the amount immediately needed to close a loan or disburse funds to a borrower.

Inaccurate Reports

We found a number of discrepancies in the organization's semiannual reports to EDA, and they did not reconcile from period to period. For example, the semiannual report dated March 31, 2004, showed 26 loans made. But beginning September 30, 2004, and continuing forward, reports show only 12 loans had actually been made. The cumulative amount of administrative expenses should have increased over time; however, the amount shown from one period to the next decreased at times. These errors cast doubt on the accuracy of all the RLF data, including the amount of excess cash.

What We Recommended

We recommended that the EDA Chicago regional director require the community development organization to place $419,655 in excessive cash reserves in an interest-bearing account and remit the interest earned to the U.S. Treasury. We also recommended that EDA deobligate $199,432 of undisbursed grant funds, require $142,018 in unallowable interest expense be returned to the RLF, and take back $29,567 in excess grant disbursements. Finally, EDA should require the organization to correct its most current semiannual report.

Grantee Response

In its response to our draft audit report, the community development corporation agreed with all of our findings and stated it would take the actions we recommended. *(Denver Regional Office of Audits: DEN-17932)*

Three California Audits Show Mixed Results

During this semiannual period, the Office of Audits reviewed EDA grants in three California localities suffering from economic stress. Although all three grantees completed their public works construction projects satisfactorily, none had made significant progress toward expected long-term economic development.

Audit Finds California Business Park Grantee Complied with Terms

In early 2000, EDA awarded a California city a $3.8 million public works grant under Title II of the Public Works and Economic Development Act to fund infrastructure at a research and technology business park. The award period extended from February 2000 to January 31, 2004. The federal share was $2,794,000, and the local match was $1 million.

The city is located in central Fresno County and agriculture is the dominant element in the local economy. Fresno County had the largest number of welfare recipients of all central California counties, and with an unemployment rate that consistently hovered in double digits in the 1980s and 1990s, it needed thousands of new jobs. The city had proposed to create a business park and recruit industries geared toward research, technology, and manufacturing to provide jobs for people from a wide geographical area. The specific project included widening roads, installing curb-and-gutter and utilities, extending water and sewer lines, and installing storm drains. When construction bids came in lower than anticipated, the city requested and EDA approved an award amendment that extended the originally approved roadway improvements beyond the limits defined in the original grant application.

This is one of two new buildings in the research and technology business park being developed by a California city to help alleviate unemployment. The EDA grant funded infrastructure for the park.

Source: OIG

We conducted a final performance audit of the award to determine whether costs claimed were reasonable, allowable, and allocable to the sponsored project; whether award objectives had been achieved; and whether accounting, procurement, and project management practices and controls complied with award requirements.

Our Findings

We found the costs claimed under the EDA award were reasonable and allowable and that infrastructure improvements had been completed as intended. But although years have passed since construction was completed and the award was closed, the park remains nearly vacant.

However, the city has an active marketing strategy involving a variety of venues and has demonstrated continued commitment to park expansion. Recently, we followed up with a visit to the park and found development on two park parcels. The city's efforts meet the intent of the EDA project, and we have determined the city complied with the terms and conditions of the award.

We had no negative findings and did not recommend any corrective actions for the city or EDA. *(Seattle Regional Office of Audits: STL-17578)*

California City Handled Grant Well but More Work Needed to Meet Economic Goals

In April 2001, EDA awarded a California city a $5 million grant to construct a regional vocational training center intended to teach residents new skills and reduce reliance on agriculture. The original award consisted of a federal share not to exceed $3.25 million and a local match of $1.75 million. The award was subsequently amended four times. The third amendment increased total estimated project costs to $5,420,101, with the federal share standing at $3.25 million but the local share being increased $2,170,101. The award period extended through August 2004.

The city had always relied on farming products such as grapes and oranges for its economic base, but after decades of economic setbacks, the locality ended up with a 15.9 percent unemployment rate by 2000. The training center was to provide remedial education, specific training, and retraining for adults looking to enter the job market. It also was intended to work with the private industry council[12] and local employers to develop job-specific training programs.

[12] Private industry councils were formed under the Job Training Partnership Act of 1982 and replaced in July 2000 by broad-mandated Workforce Invest Boards. The councils planned job training and employment service programs and conducted oversight in cooperation with local elected officials.

The California city using an EDA grant to build a regional vocational training center finished the second floor only to "vanilla shell" stage, which reduced the building's training capacity.

Source: OIG

We conducted a final performance audit of the award to determine whether costs claimed under the EDA award were reasonable, allowable, and allocable to the project, and whether grant objectives were achieved. We also wanted to determine if accounting, procurement, and project management practices and controls complied with award requirements, assured efficient grant administration, and resulted in an acceptable final project.

Our Findings

We found that the costs claimed under the award were reasonable, allowable, and allocable to the project, and the city had complied with the basic terms and conditions of the award. The city constructed its regional vocational training center, but by April 2006 when we performed our audit, nearly 2 years after the award ended, the economic benefits expected of the project had yet to fully materialize.

Because of escalating construction cost estimates, the city did not complete the second floor of the center. With EDA's approval, the building was finished only to "vanilla shell" stage, which effectively reduced the center's training capacity by half. A vanilla shell is a completed external structure with minimal interior partitioning walls, paint, or floor covering. The city did not adjust its performance targets to account for the reduced capacity. The city also did not have a system for identifying and tracking training accomplishments and progress or a strategic marketing plan to meet its economic development goals.

The city had taken some steps to promote the center by assigning center responsibility to an administrator who worked with individuals and businesses in the community. Most center promotion and management duties were assigned to the city's administrative services director who spent half her time on center-related activi-

ties in addition to her primary duties of managing city budgeting and grants, financial services, and human resources.

In mid-2005, the city also convened a site committee to promote the center and a marketing committee to inform the public of services available from its tenants. Center tenants provide a number of training courses and programs, but the city was unable to provide evidence that these courses are part of an orchestrated curriculum designed to lead to nonagricultural jobs. Without a student profiling and job tracking system and a documented curriculum, there is no way to be sure the center's training programs are systematically migrating students from agricultural employment to new job fields.

Our Recommendations

We recommend EDA require the city to revise the project performance goals because of the center's reduced capacity, implement a system for tracking and reporting center training accomplishments, and develop a strategic marketing plan to define, organize, and solidify the city's marketing vision. The plan should include time frames and milestones and identify target student categories and prospective training vendors. The city also should develop and document the assigned responsibilities for marketing, managing, and operating the center.

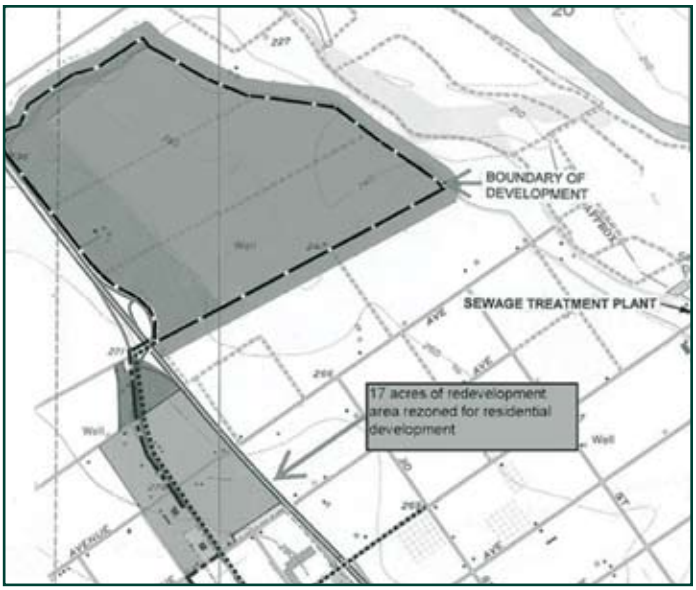
Grantee Response

Overall, city officials concurred with our findings and recommendations and described for us the corrective actions they had taken or that were in progress. We eliminated one finding in the report based on the city's evidence that it had taken required corrective action in response to our draft report. We encouraged the city to seek guidance from and coordinate its ongoing corrective actions with EDA to ensure they are properly completed. *(Seattle Regional Office of Audits: STL-17579)*

Audit Finds California Water and Sewer Project Performance Deficient

In 2001, EDA awarded a $3.2 million grant to a California county and adjacent city for a water and sewer project to build 7,400 linear feet of sewer lines and 4,800 linear feet of water lines to connect city utility systems to two large parcels of property. The award included a federal share of $2.2 million (70 percent) and a local match of $986,000 (30 percent). After amendments, the award was extended to November 30, 2004.

The 217.5-acre project consisted of two privately owned properties: a 106.5-acre redevelopment project zoned for light industrial and commercial use inside the city limits and a 111-acre parcel in the county to be developed as an airplane museum, a recreational vehicle (RV) park, hotel, fast food restaurants, spa, and winery. Local officials believed the proposed developments would generate 400 or more jobs in tourism-related businesses anticipated to cluster on the lands serviced by the project improvements.



This schematic shows the development area where two California localities used an EDA grant to extend water and sewer utilities to two privately owned properties. The lands are being developed as an airplane museum, RV park, hotel, fast food restaurants, spa, and winery to generate 400 jobs.

Source: OIG

We conducted a final performance audit to determine whether costs claimed under the EDA award were reasonable, allowable, and allocable; whether award objectives were achieved; and if the project's accounting, procurement, and project management practices were proper. Our audit revealed the city's performance was deficient in several ways:

$130,692 Is Due to the Government

Our review disclosed that the city failed to ensure that its administration of the grant adhered to applicable federal cost principles and uniform administrative requirements. We questioned $186,702 of $2,832,834 in claimed costs and we recommended recovery of the federal share of $130,692.

Project Was Built, Economic Benefits Did Not Come

Before the infrastructure project was complete, the city rezoned 11.77 acres of the 106.5-acre redevelopment area from light industrial and commercial to residential, which reduced the

acreage available to generate the predicted long-term economic development.

At the time of our audit in August 2005, a year had passed since construction was completed and the 111-acre tract in the unincorporated area of Monterey County that belonged to the prime project beneficiary was still vacant. When we followed up in August 2006, the project was still undeveloped, and its county development permit was set to expire in October 2006. In addition, the localities did not have a viable marketing strategy in place to help meet the economic development goals.

Our Recommendations

We recommended the EDA regional director take a number of actions:

- Inform the grant recipients that the remaining redevelopment property must remain zoned for light industrial and commercial use for the entire economic life of the project.
- Require the grantees to develop and implement a long-term development strategy and a comprehensive marketing plan.
- Inform the recipients of the risk of having to refund the grant and be designated "high-risk" recipients because of unsatisfactory performance.
- Disallow questioned costs of $186,702.

Grantees' Responses

In general, the recipients concurred with our findings and recommendations and described corrective actions in progress or proposed. However, the city disagreed with the number of acres rezoned from light industrial and commercial to residential use and provided support for its revised number. We accepted the city's support and have adjusted the final report and questioned costs accordingly. We did not agree with the city's assertion that a rezoning of 5 percent of the total area should not result in ineligible costs and stand by our report.

The city agreed to create and implement project development strategies that promote timely accomplishment of the long-term job generation requirements necessary to achieve the full economic potential of the project and noted that it had increased staff time devoted to the marketing and developing of the EDA project.

The county took exception to the recommendation to develop a marketing plan for private property. We appreciated that concern and encouraged EDA to ensure the county implements the safeguards proposed to protect EDA's interest. The county has agreed to recommend that the developer post a faithful performance bond, which would be used to repay a proportionate share of the grant attributable to the unincorporated portion of the utilities project if the development fails. *(Seattle Regional Office of Audits: STL-17580)*

COMMERCE
AMONG NATIONS
SHOULD BE FAIR AND
EQUITABLE — FRANKLIN

ECONOMICS AND STATISTICS ADMINISTRATION

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:

U.S. Census Bureau 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 quinquennial 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.

Group Quarters Enumeration Continues to Challenge the Census Bureau

We are closely monitoring the Census Bureau's preparations leading up to the 2010 national decennial census. In the March 2006 *Semiannual Report to Congress* (pages 19-22), we reported on the opportunities the Census Bureau missed during its test of the automated address canvassing operation with handheld computers.

The Census Bureau has reengineered its strategy for the 2010 decennial to improve accuracy, reduce risks, and contain costs. Part of that strategy includes a program of early planning, development, and site testing culminating with a 2008 dress rehearsal of the actual 2010 census. A site test is a partial census of population and housing under realistic conditions in selected areas to determine if procedures and systems are effective prior to a decennial census. The Census Bureau is conducting the 2006 test in two locations—a portion of Travis County, Texas, that includes parts of the city of Austin and its suburbs, and the Cheyenne River Reservation and Off-Reservation Trust Land in South Dakota. The bureau chose these two sites because their demographics and geography support test objectives.

Counting Group Quarters Residents Proved Difficult

Most residents in the United States live in single family houses, apartments, and mobile homes. But according to Census 2000 data, more than 7.8 million people live in situations called group quarters, such as college dormitories, nursing homes, prisons, migrant worker dormitories, convents, and group homes. Since the 1970 decennial, the bureau has used different procedures to enumerate this population, because counting group quarters differs from enumerating other types of housing units.

Enumerating group quarters in the 2006 test consisted of developing the group quarters list, validating the list to verify and define the type of group quarters, and enumerating group quarters residents. Census employees visited every address on the list to determine whether the address is actually a group quarters and, if so, what type. After validation, a final list was produced for enumeration. We conducted our review at the Travis County site, where residential housing units received a Census questionnaire in the mail. But enumerators visited each group quarters by appointment to either complete the Individual Census Report or drop it off to be filled out by residents or the group quarters administrator. Once a form for each resident had been completed and reviewed, the forms were taken to the local census office to be shipped for processing at the National Processing Center in Jeffersonville, Indiana.

We reviewed the group quarters operations in Austin to determine (1) whether the recommendations made by internal and external evaluations following the 2000 Census and 2004 test for the 2010 decennial were addressed, (2) whether there were new or continuing problems in the operation, and (3) whether all existing group quarters in the test area had been identified and enumerated. Although the bureau is clearly testing new methods to better enumerate the group quarters population, we concluded that it still has a number of problems to overcome in enumerating group quarters.

Census Addressed Many Group Quarters Problems from 2004 but 2006 Test Revealed New Ones

After the 2000 decennial census and the 2004 census test, a number of operational assessments and evaluations were issued by the Census Bureau, the National Research Council of the National Academy of Sciences, the Government Accountability Office, and the Office of Inspector General. We found the bureau addressed most of those recommendations including attempting to improve the group quarters list and reduce list duplication, revising group quarters definitions and the group quarters questionnaire, better tracking of the group quarters questionnaire, and counting people where they sleep (as in dorms) rather than where administrative records are kept (e.g., University of Texas).

The Travis county site includes four large universities and colleges, making it an ideal test site for the student population. But students proved a particularly challenging population for enumerators, especially those living in fraternities and sororities. We recommended Census find better ways to count students living in college/university group quarters, such as using campus resources (e.g., student Greek life offices) to obtain administrative records for fraternity/sorority students.

Incorrect Designations Hampered Enumeration

During the 2006 Census test, the group quarters list-building activities identified 1,778 addresses to be verified as a group quarters, housing unit, or nonresidential address. We reviewed more than 1,500 validation questionnaires and discovered that some residents and managers of nontraditional student housing, such as private dorms and student cooperative housing, self-identified themselves as a group quarters facility even though they did not fit into any of Census's group quarters definitions. As a result, the number of facilities and population counts for that type of group quarters is likely inaccurate.

Census uses a database program to select every 10th group quarters for a quality check. Batch envelopes not checked for quality are placed in a checkout box. Then the envelopes and records are rescanned and shipped out to Jeffersonville, Indiana.

Source: OIG

Small residential group quarters often blend into single family neighborhoods. This ordinary looking house in Austin turned out to be a convent.

Source: OIG

If these nontraditional student housing units were defined as private residences that received housing unit questionnaires, there was an increased likelihood that students who did not respond had moved out of their residence prior to the follow-up operation. In those cases, enumerators relied on records kept in administrative offices, which often lacked Hispanic origin and race information. It took more time and effort to enumerate these facilities than if the building had originally been defined as a group quarters.

Apartment Complexes Were Incorrectly Identified

We found that 42 percent of the 1,778 addresses to be validated were associated with large apartment complexes. During address canvassing, individual apartments in large complexes were erroneously identified as potential group quarters. This consumed an inordinate amount of lister and enumerator time, wasted resources (such as other living quarters validation questionnaires), and antagonized apartment managers by having several enumerators visit them multiple times. The processes used to enumerate large apartment complexes appear unwieldy, although Census has identified a change that will reduce the number of enumerators visiting an apartment complex.

Final List Did Not Include More Than a Dozen Existing Group Quarters

The validation operation was supposed to refine the list into a final group quarters enumeration list. But we found an additional 15 group quarters that had not been included on the list just by doing a limited Internet search, something that had been recommended after the 2000 Census, and speaking with group home administrators. We also found three facilities that appeared twice on the list and six addresses on both the group quarters enumeration and housing unit lists, which could cause inaccurate counts.

Census's oversight and evaluation methods do not adequately address the problems associated with the group quarters validation and enumeration lists. Census should use online tools (e.g., state licensing web sites) to identify additional group quarters facilities and do a better job of verifying lists.

Census Needs to Improve Some of the Administrative Procedures of the Group Quarters Operation

We found some group quarters enumeration processes and procedures that should be improved in preparation for the 2008 dress rehearsal and the 2010 decennial. For example, during the 2000 census, some forms were unaccounted for or could not be associated with a particular group quarters. The bureau implemented a procedure to scan all forms when they arrived at the local Census office and then scan them again when they were shipped out to the National Processing Center. This ensured forms could be returned to the correct batches if they were inadvertently separated.

However, scanning every form twice will increase the document scanning workload in the 2010 census by at least 15 million over the 2000 local Census office workload and may not be necessary if the forms and batch envelopes are unopened from the time they were scanned in to the time they are shipped. We recommended the bureau find a way to more efficiently track the forms, such as using a sealed envelope system.

Bureau Response

The Census Bureau concurred with some of our findings and recommendations, but took issue with others. In particular, the bureau believes that its quality assurance methods to identify, quantify, and rectify problems are sufficient. The bureau also disagrees with exploring the use of the Internet as a possible response option for campus student enumeration. In light of the results of Census 2000 and three other tests of responding online, the bureau has eliminated the Internet option because of low usage, increased security risk of census data, and high implementation costs. However, we had suggested only that the bureau explore using the Internet to contact a small, specific population — students — via e-mail and allow them the option to respond electronically. The bureau did agree with our recommendation to use the Internet and other resources to improve the group quarters list.

Census also did not agree with our finding that the double scanning process for the group quarters enumeration forms was unnecessary except for those that were opened for quality control. The bureau only partially agreed to review and revise, as necessary, the methods used to evaluate the accuracy of and reduce duplications on the group quarters list. We asked Census to provide us with additional support and reasoning in an action plan. *(Office of Inspections and Program Evaluations: IPE-18046)*

The local Census office clerk scans the barcode label on each batch envelope of forms in the check-in box, then scans the barcode of each individual record in the envelope.

Source: OIG

Audits Unresolved for More Than 6 Months

ITS Services, Inc.

In March 2005, we reported that 3 of the 32 task orders awarded under a Virginia IT services contract were audited to determine whether the costs billed by the firm were reasonable, allowable, and allocable under contract terms and conditions and federal regulations. We found that the firm had failed to comply with numerous contract and federal requirements, and we questioned more than $8.5 million in direct labor and reimbursable costs.

Computer & High Tech Management, Inc.

We reported in our September 2005 *Semiannual Report* (page 14) the results of audits of 2 of the 21 task orders for another Virginia firm providing IT services to Census. We sought to determine whether the firm had complied with contract terms and conditions and federal regulations and had billed Census for work performed in accordance with specifications of the task order. We found that the firm failed to comply with numerous contract and federal requirements, which caused us to question more than $10.7 million in direct labor and other reimbursable costs.

We have suspended audit resolution on both of these contract audits pursuant to an agreement with Census.

INTERNATIONAL TRADE ADMINISTRATION

The **International Trade Administration** is responsible for trade promotion and policy issues associated with most nonagricultural goods and services. ITA works with the Office of the U.S. Trade Representative to coordinate U.S. trade policy and with other agencies to coordinate U.S. trade promotion efforts. ITA has four principal units:

Market Access and Compliance develops and implements international economic policies of a bilateral, multilateral, or regional nature, and participates in trade negotiations. Its main objectives are to obtain market access for American firms and workers and to ensure full compliance by foreign nations with trade agreements signed with the United States.

Manufacturing and Services undertakes industry trade analysis, shapes U.S. trade policy, participates in trade negotiations, organizes trade capacity-building programs, and evaluates the impact of domestic and international economic and regulatory policies on U.S. manufacturers and service industries.

Import Administration defends American industry against injurious and unfair trade practices by administering the antidumping and countervailing duty laws of the United States and enforcing other trade laws and agreements negotiated to address such trade practices.

U.S. Commercial Service seeks to promote economic prosperity, enhance U.S. job creation, and strengthen national security through a global network of international trade professionals. CS promotes and protects U.S. commercial interests abroad and delivers customized solutions to help U.S. businesses, especially small and medium-sized enterprises, compete effectively in the global marketplace.

ITA's Commercial Service Operations in Argentina and Uruguay Operate Well, but Financial Processes Need Attention

Commerce OIG regularly inspects U.S. Commercial Service (CS) overseas posts. In late 2005, we inspected the five CS China offices. Our report, *CS China Generally Performs Well but Opportunities Exist for Commerce to Better Coordinate Its Multiple China Operations* (IPE-17546), was profiled in the March 2006 *Semiannual Report to Congress* (pages 23-26).

In June 2006, we inspected CS' offices in Argentina and Uruguay, focusing on management, program operations, and financial and administrative practices. These offices have a combined management structure, both being managed by the senior commercial officer in Argentina. CS' staff in Uruguay also coordinates with the State Department economic counselor in Uruguay on day-to-day matters.

Our review found that CS Argentina and CS Uruguay are providing useful export assistance to U.S. companies and have established collaborative relationships with key U.S. government offices and nongovernmental organizations. CS Argentina's River Plate regional initiative promotes the Uruguay market to U.S. exporters, and the office collaborates effectively on export control activities with Commerce's Bureau of Industry and Security.

Posts Have Effective Administration, but Face Future Challenges

Both posts generally work well. During FYs 2005 and 2006, feedback from CS Argentina and CS Uruguay's clients was generally positive. Most clients said they were satisfied with the quality and timeliness of the services they received. CS Argentina's management of human resources, physical office space, information technology, and other administrative matters is effective overall. However, we found a few concerns at both posts that warrant management action.

Property management, particularly in Uruguay, needs improvement. We recommended CS improve guidance on property and inventory management, including the disposal of computers and other property so that both posts can properly dispose of obsolete and surplus items.

CS Argentina also needs to plan ahead for the approaching retirements of its senior commercial specialists. Both CS Argentina and CS Uruguay should develop effective partnerships with Commerce's Brazil-based regional programs to promote compatible technical standards and intellectual property rights protection.

Posts Should Improve Documentation of Export Successes

Since CS' handling of this important performance measurement has been a recurring problem over the last several years, we reviewed a sample of the export successes reported by both posts during FYs 2005 and 2006. We found that most of the reported successes complied with most aspects of CS' export success guidance, and the narratives describing the export successes generally contained sufficient detail. CS officers did review all reported export successes and did verify the pertinent facts for some of the reported transactions. But the posts did not always maintain sufficient documentation to fully substantiate reported export transactions and CS' value-added export-related assistance.

The posts were able to provide full documentation substantiating only 49 percent of the export successes in our sample and partial documentation for another 34 percent of the sample. There was no documentation for the remaining 17 percent. We recommended CS Argentina management comply with CS' export success guidelines, which require posts to retain documentation verifying the accuracy of reported successes.

2005 Country Profiles

Argentina

Population: 39.9 million

Size: 1.07 million sq. mi.

GDP: $518 billion purchasing power parity

Major industries: consumer durables, chemicals and petrochemicals, food processing, motor vehicles, metallurgy, and textiles

Leading agricultural exports: fruits, corn, tobacco, peanuts, wheat, and livestock

Leading sectors for U.S. exports and investment: agricultural machinery, electric power systems, information technology, medical equipment and supplies, and mining machinery

Uruguay

Population: 3.4 million

Size: 68,040 sq. mi.

GDP: $32.9 billion purchasing power parity

Major industries: beverages, chemicals, electrical machinery, food processing, petroleum products, and textiles

Leading agricultural exports: barley, corn, fish, livestock, rice, and wheat

Leading sectors for U.S. exports and investment: agriculture, chemicals, telecommunications, fertilizers, and infrastructure projects

Sources: CIA World Fact Book (2006) and CS Argentina's *Country Commercial Guide* 2006, and CS Uruguay's *Country Commercial Guide 2006*

Accounting and Financial Management Need Attention

CS management had requested that we review the advantages and disadvantages of CS Argentina's current process of certifying its own payments in Argentina. Specifically, CS management sought more information on the process in Argentina as it considered whether it should seek to have other posts certify their payments in order to reduce charges for administrative services provided by the State Department.

In 2000 CS Argentina partially opted out of the State Department's payment certification and accounting services. We found that CS slightly reduced the amount that it pays to the State Department by certifying its own vouchers, but current ITA and Commerce policies prohibit this. Select CS Argentina staff who were certifying payments when we inspected the post, though trained, were not properly authorized to do so. CS headquarters permitted certification of payments but did not have the authority to make that decision.

We also found that CS Argentina does not receive full accounting services from the State Department. This may compromise Commerce's internal controls for overseas accounting because ITA's accounting practices partially rely on the State Department's internal control procedures to verify the overseas transactions reported to ITA through State's accounting system. CS Argentina's accounting procedures are also inconsistent with ITA policy, as clarified by ITA during the course of our review. That policy requires overseas posts to receive their accounting services from the State Department.

We recommended CS change its financial management practices in Argentina to comply with ITA and Commerce policies. CS headquarters should coordinate any future financial management initiatives with ITA to ensure that the initiatives are permitted and have adequate controls and oversight. CS headquarters and ITA's Office of Financial Management should also improve their coordination and communication to ensure that all CS officials at headquarters and posts understand overseas financial management policies.

Bureau Response

ITA agreed with most of our findings and provided responses detailing actions it will take to correct problems we found. The initial response represents a positive step, but we have asked ITA to take additional steps to adequately respond to our recommendations. For example, ITA's response said that the May 18, 2006, changes

to its export success verification and documentation guidance were made to establish clear standards for export success claims. However, that guidance was not clear on verification methods to be used by first-level approvers of export successes. CS has since issued more detailed export success verification procedures that adequately address our concerns.

ITA stated that CS Argentina has discontinued the practice of certifying its own payments. However, CS Argentina's partial participation in State's accounting services calls into question the effectiveness of internal controls for accounting at overseas posts. ITA must either ensure that the accounting services provided by State for CS Argentina are consistent with established internal controls for overseas posts, or it must establish separate oversight processes for the post. Since the release of our final report, CS has reported to us that it has fully subscribed to the State Department's accounting services.

ITA did not agree that CS Uruguay should transfer user fees that it collects for services provided by the State Department back to that department. ITA said the spirit of cooperation between the Commerce and State staffs in Uruguay "could be damaged by a new emphasis on division of collections." Despite this close working relationship, CS does not have the authority to retain user fees that it collects for the State Department. CS should develop procedures consistent with applicable rules on user fees and similar to procedures followed for collections at other partnership posts.

Source: http://www.cdc.gov/travel/images/map_temsam.jpg

ITA's response said authority to dispose of property is granted via e-mail messages from regional offices, but those instructions are not consistent with guidance provided in the Office of International Operations *Administrative Manual*. Providing accurate guidelines for securing information technology assets is necessary to protect sensitive information stored on government computers, handheld devices, and other equipment. *(Office of Inspections and Program Evaluations: IPE-18111)*

OIG Makes Recommendations to Improve Travel Briefings

After learning Commerce employees were not routinely receiving formal counterintelligence briefings prior to traveling to certain foreign countries, we held a number of discussions with the director for security and other senior officials from the Office of Security. We also issued a report with recommendations we believe would improve the process. Department officials responded with only partial agreement to our suggested improvements. In May 2006, we met with Department officials again. As a result, we modified some of our recommendations, but we requested an action plan within 60 days. That action plan has now been submitted by the Office of Security and is under review. We will continue to monitor the issue to ensure all Commerce travelers receive appropriate counterintelligence preparation prior to going overseas on official business. *(Office of Inspections and Program Evaluations: IPE-17954)*

Suitability Review Process Needs Improvements

During this semiannual period, we conducted a classified examination of Commerce's review process that determines the suitability of staff assigned to certain overseas posts. We recommended that ITA and Commerce's Office of Security better define the procedures and coordinate the timing of such reviews. *(Office of Inspections and Program Evaluations: IPE-17546, Appendix F)*

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 provides products, services, and information that promote safe navigation, support coastal communities, sustain marine ecosystems, and mitigate coastal hazards.

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 Great Lakes, 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 uniformed service.

Soaring Costs, Delays Plague Triagency Satellite Program

The National Polar-orbiting Operational Environmental Satellite System (NPOESS), a joint project of NOAA, Defense, and NASA, is intended to monitor global environmental conditions and disseminate climate data to support military, civilian, and scientific needs. NPOESS will combine existing polar-orbiting satellites into a single state-of-the-art system.[13] NOAA has overall management responsibility for the converged system; Defense is the lead on acquisition matters; and NASA is the lead for promoting transition to new technologies.

NPOESS' original acquisition plans entailed, among other things, development of seven instruments under a single satellite integration contract worth $4.5 billion awarded to a prime contractor. The contract included an incentive arrangement that made it possible for the contractor to be paid lucrative bonuses ("award fees") of as much as 20 percent of the total estimated contract cost. Initial estimates put life-cycle costs for the entire system at $6.5 billion and set a deadline of March 2008 for the first satellite launch.

In September 2005, satellite program officials notified Congress that NPOESS costs had grown by at least 15 percent, largely because of problems with the Visible/Infrared Imager Radiometer Suite (VIIRS)[14]—one of four sensors considered critical to the program. In November 2005, the Government Accountability Office (GAO) informed Congress that life-cycle cost estimates for NPOESS were likely to grow to $9.7 billion, and the launch of the first NPOESS satellite was at least 17 months behind schedule.[15] That same month, DoD's Cost Analysis Improvement Group estimated that NPOESS cost growth had exceeded 25 percent, triggering the Nunn-McCurdy provision of the 1982 National Defense Authorization Act. Nunn-McCurdy requires the Defense Secretary to certify in writing that the program is essential to national security; an alternative, less costly option does not exist; new cost estimates have been developed and are reasonable; and a management structure is in place to keep costs in check. Without such certification, DoD's involvement in the program would be terminated and program funding cut in half.

NPOESS was at this point some $3 billion over budget and well behind schedule, yet the contractor had received more than $123 million—*84 percent*—of available award fees. Our audit sought to determine how cost and schedule overruns had grown to such proportions without apparent penalty to the contractor. We

[13] In 1994, by Presidential Decision Directive, NOAA merged its Polar Operational Environmental Satellite (POES) Program with the Department of Defense's Defense Meteorological Satellite Program to produce the National Polar-orbiting Operational Environmental Satellite System (NPOESS).

[14] VIIRS collects visible/infrared imagery and radiometric data, such as sea-surface temperature readings and ocean color measurements.

[15] U.S. Government Accountability Office, November 2005. *Polar-Orbiting Environmental Satellites—Technical Problems, Cost Increases, and Schedule Delays Trigger Need for Difficult Trade-off Decisions,* GAO-06-249T. Washington, D.C: GAO.

looked at how the contractor identifies and communicates problems with NPOESS to the integrated program office—the entity within NOAA responsible for day-to-day management of the satellite program; how that office in turn communicates problems to NOAA officials; and whether award fees allowed under the integration contract were administered effectively.

Major Findings

We uncovered two overarching management and contract weaknesses that contributed to the unchecked cost and schedule overruns.

The NPOESS Executive Committee Did Not Challenge Optimistic Assessments of the Impact of VIIRS Problems

Reports that problems with the VIIRS sensor would delay the NPOESS launch took observers of the program by surprise, prompting our concerns that the integrated program office either was unaware of the VIIRS problems or failed to bring them to the attention of senior management, particularly the NPOESS executive committee (EXCOM). EXCOM is made up of top leadership from each agency: the Under Secretary of Commerce for Oceans and Atmosphere, the Under Secretary of Defense for Acquisition and Technology, and the NASA Deputy Administrator.

In fact, we found that information sharing was not effective between the contractor, the VIIRS subcontractor, and the program office at the outset of the program. But as VIIRS problems persisted, the program office and prime contractor took steps to improve communication and increase oversight of the VIIRS subcontractor. Beginning in December 2002, the integrated program office submitted monthly status reports to EXCOM that explicitly described the growing costs and delays attributable to VIIRS. Yet until March 2005 the program director—a NOAA employee—maintained that these problems would be solved within available funding reserves and that NPOESS remained on schedule.

Despite mounting evidence of the seriousness of the VIIRS problems, EXCOM did not challenge the director's optimistic assessments, and rarely convened during the first years of the program to consider its status. Finally, in 2005, after the program office reported that VIIRS problems would indeed delay the first satellite launch, EXCOM began meeting more often to investigate the issues and their impact. Unfortunately, by then it was too late to turn the program around: EXCOM's long-term inattention had, in effect, postponed critical evaluations and decisions needed to replan the program's faltering elements and contain cost and schedule overruns.

Under the revamped NPOESS program, the U.S. will launch four orbiters instead of six, and rely on European satellites to fill any resulting gaps in satellite coverage.

Source: http://eic.ipo.noaa.gov/IPOarchive/ED/graphics_kit/npoess_orbiter_300DPI.jpg

We recommended that the Deputy Secretary ensure the Under Secretary for Oceans and Atmosphere works with the other members of EXCOM to obtain regular, independent evaluations of the status of NPOESS that thoroughly assess progress toward completing critical tasks.

Contractor Received Excessive Award Fees

Award fees are supposed to motivate a contractor to strive for excellence. But the NPOESS experience shows that this incentive structure does not always result in the intended caliber of performance. Despite ongoing, significant delays and cost overruns, the prime contractor received close to the maximum fee amounts for the first five billing periods—an average 90 percent of available incentive payments. It was only in period six—which covered the 6 months prior to the Nunn-McCurdy breach—that the contractor's performance was rated unsatisfactory. Even so, the prime received 48 percent of the potential fee amount—$10.7 million.

These payments were permissible because the award fee plan's evaluation criteria do not sufficiently tie incentive earnings to

completion of the most critical or high-risk tasks. And the potential fee pool—20 percent of total estimated costs—is atypical: a GAO review of Defense award fee contracts found that less than 1 percent of these arrangements allowed fee pools to exceed 15 percent of estimated costs. Finally, the NPOESS plan gives total authority for setting fee amounts to a "fee determining official" who in the case of NPOESS is also the program director. This individual's objectivity in assessing the contractor may well be compromised by his responsibility for NPOESS' day-to-day management and his stake in the program's success. The payments approved by the fee determining official for periods two through five routinely exceeded the recommendations made by the NPOESS review board.

The Under Secretary for Oceans and Atmosphere and his EXCOM counterparts should revise the NPOESS award fee plan to (1) tie incentive payments to the most critical tasks and contractor performance, and (2) assign responsibility for determining fee awards to an official who does not directly manage the program.

Responses from the Department and NOAA

In responding to our report, the Deputy Secretary of Commerce stressed the importance of NPOESS to the Department's mission and national responsibilities, noting that he now receives monthly NPOESS progress reports from NOAA. He stated that he will work with the Under Secretary for Oceans and Atmosphere and the EXCOM partners to ensure NPOESS is managed, operated, and monitored in a way that meets the intent of our recommendations as well as those of the Nunn-McCurdy process.

The Under Secretary for Oceans and Atmosphere generally agreed with the intent of our recommendations but stated that the report does not (1) adequately acknowledge the complexity of the NPOESS program, (2) represent the ongoing level of EXCOM's direct involvement in overseeing both NPOESS and the integrated program office, (3) fully characterize the contract's award fee structure, and (4) adequately recognize Defense's role in administering the contract.

We assessed our report in light of NOAA's comments and determined that it did in fact present in enough detail the information NOAA believed was lacking. We worked with NOAA to develop a suitable action plan for resolving the weaknesses we identified. *(Offices of Audits and Systems Evaluation: OIG-17794)*

Search and Rescue Satellite System Does Not Provide Adequate Assurance of Users' Identities

The security of information exchanged over the Internet is critical to the effectiveness of e-government operations and to the public's willingness to use online government services. OMB requires agencies to formally assess the degree to which this information must be protected. These risk assessments measure the harm that would result from the data's unauthorized release or modification. The level of harm dictates the level of "assurance," or confidence, in a user's identity a system must establish before allowing access and determines how rigorous the electronic authentication process for verifying user identities must be. We evaluated the quality of an assessment NOAA conducted on the e-authentication process that controls user access to its Search and Rescue Satellite-Aided Tracking system (SARSAT).

SARSAT is the U.S. portion of an international search and rescue program. It collects emergency information that is transmitted from beacons carried on ships, planes, and search and rescue personnel to satellites. The information is then sent to the appropriate

Life-saving SARSAT operations begin with distress signals transmitted from beacons carried by people, planes, or ships to the global network of search and rescue satellites. The personal locator beacons pictured here use GPS technology to alert rescue personnel within 3 minutes of signal transmission.

Source: http://www.noaanews.noaa.gov/stories/images/plb-groupshot2.jpg
http://www.omao.noaa.gov/aviationsafety/pdf/AviationLifeSupportEquipmentProgram.pdf#search=%22SARSAT%20beacons%22

U.S.-based rescue coordination centers and international entities. SARSAT maintains databases of registered beacons and incident histories, both accessible to authorized users via web-based applications.

Our evaluation sought to determine if the SARSAT risk assessment identified the appropriate level of e-authentication controls and whether the controls had been implemented and properly certified prior to the system's accreditation.

Determining E-Authentication Needs

OMB established four assurance levels for agency applications, depending on the business being conducted, with level 1 requiring little or no confidence in the user's identity and level 4 requiring very high confidence. The risk assessment measures the potential adverse impact on individuals or an organization's operations or assets in six categories: inconvenience, financial loss, harm to agency programs, unauthorized release of sensitive information, personal safety, and criminal or civil violations. Each assurance level correlates with specific control requirements established by the National Institute of Standards and Technology in NIST Special Publication 800-63, *Electronic Authentication Guideline*.

Responding to a distress signal picked up by SARSAT, a U.S. Coast Guard helicopter airlifts the stranded crew of a grounded ship off the coast of Texas.

Source: http://www.sarsat.noaa.gov/

Once the risk assessment has determined the level of confidence, agencies must prepare system security plans that fully document requirements for authenticating users and the controls they have planned or in place for doing so. They must test controls and have them independently certified prior to the system's accreditation, develop a plan of action for eliminating the deficiencies, and set milestones for tracking and monitoring their resolution. They must submit to the official responsible for authorizing a system's operation, a security assessment report that describes the extent to which controls are implemented correctly, operating as intended, and meeting security requirements.

SARSAT's E-Authentication Controls Fall Short

We found problems with SARSAT's e-authentication risk assessment and system security plan, and found that certification activities did not appropriately examine e-authentication controls. We also identified unmitigated deficiencies in the controls for the web applications.

NOAA Did Not Accurately Assess Assurance Levels

Agencies determine required assurance levels by comparing the impact profile from their risk assessment with impact profiles in OMB's guidance, and selecting the level that meets or exceeds the potential impact to their system in every category. For example, if an agency determines an authentication error could have a moderate or high impact on personal safety, it should meet level 4 e-authentication requirements, even if all other consequences are minimal.

For one of the SARSAT databases, the risk assessment rated the potential impact of unauthorized access to *personal safety* as moderate. But NOAA assigned an assurance level of 2 for both databases, rather than level 4, as OMB requires.

The assessment incorrectly assigned a *low* level for the impact category *unauthorized release of sensitive information*: beacon registration data is protected under the Privacy Act, and as such requires a higher impact rating. The SARSAT system security plan, in keeping with Privacy Act requirements, describes a *moderate* level of impact from breaches in the confidentiality of this information. Because the assessment incorrectly considered confidentiality objectives for beacon registration information, assurance levels were miscalculated and the risk to data in both applications was mischaracterized. The assessment failed to provide any justification for the lower assurance levels.

Finally, OMB guidance requires agencies to (1) consult with their office of counsel regarding legal issues that may impact authentication requirements, and (2) consider the risk posed by users' denial (or repudiation) of having electronically transmitted or received information. We found no evidence of legal consultation in SARSAT's risk assessment, and scant consideration of nonrepudiation.

The System Security Plan Did Not Adequately Address E-Authentication Controls

A system security plan should provide an overview of security requirements, including those for e-authentication, and detail the controls that are in place or planned for meeting them before the system is authorized to operate. The SARSAT security plan did not address these requirements, and did not adequately explain the established or planned authentication controls.

For example, level 2 systems must have an identity-proofing process that validates enough information to uniquely identify new users. The SARSAT plan did not describe such a process, and the system security officer confirmed that identity proofing does not occur. The security plan also did not detail mechanisms for authenticating web-based users. OMB does allow agencies to reduce control requirements given certain cost/benefit considerations, but they must justify their decisions to do so. NOAA's system accreditation package contained no such justification. At present, the controls in place for the web applications fail to meet even level 1 requirements. In addition, a login vulnerability in one of the web applications identified by the risk assessment had not been corrected, and our own examination of the other web application revealed the same vulnerability.

The plan's failure to document requirements and controls resulted in inadequate system certification: e-authentication controls were not sufficiently tested, the security assessment report was incomplete, and the authorizing official was not informed of e-authentication deficiencies that may, in fact, increase the risk of harm to both individuals and agency operations.

Recommendations and NOAA Response

We recommended that NOAA, among other things, redo the e-authentication risk assessment to address the shortcomings we identified and improve the system security plan; correct vulnerabilities in the web applications' login processes; and test e-authentication controls, document deficiencies, and track their resolution.

NOAA disagreed with our conclusion that SARSAT's e-authentication controls do not provide adequate assurance of users' identities, but accepted all but one of our recommendations (after we clarified the meaning of one of them). NOAA reported that it has already corrected the login vulnerabilities we identified. The agency plans to (1) update the e-authentication risk assessment and include justification for why it did not implement minimum e-authentication controls; (2) revise the system security plan in accordance with NIST SP 800-53 requirements; (3) test SARSAT e-authentication controls; and (4) track gaps between required and implemented controls. *(Office of Systems Evaluation: OSE-18020)*

FISMA Review Reveals Officials Need More Information for C&A Decisions

As a part of our FY 2005 Federal Information Security Management Act reporting, we evaluated two important parts of NOAA's certification and accreditation process: (1) system security plans/risk assessments, and (2) security control assessments. Although our report details findings from work NOAA did in FY 2005, it was issued because our preliminary review of five C&A packages earlier in FY 2006 revealed that these packages had similar problems.

On February 24, 2005, the Department's chief information officer issued a plan to have improved C&A packages by the end of FY 2005 for all national-critical systems, along with a substantial number of mission-critical systems, as a way to eliminate Commerce's IT security material weakness. All Commerce systems were to have acceptable C&A packages by the end of FY 2006. Accordingly, in FY 2005, NOAA began an effort to improve its certification and accreditation process.

For FY 2005, we reviewed the C&A documentation for three NOAA systems: the Search and Rescue Satellite-Aided Tracking system, the Polar Operational Environmental Satellite Ground System (POES), and the Office of Response and Restoration Seattle Local Area Network (Seattle LAN). Each of these systems was certified and accredited as part of NOAA's C&A improvement effort.

What Is C&A and Why Does It Matter?

Certification is a comprehensive assessment of security controls implemented in a computer system. It documents whether controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Through the formal assessment of controls, the system certifier identifies any vulnerabilities that have not been eliminated by security controls.

Accreditation is management's formal authorization to allow a system to operate. It includes an explicit acceptance of the risks posed by any identified remaining vulnerabilities. Through accreditation, senior agency officials take responsibility for the security of systems they manage and for any adverse impacts should a breach in security occur.

In 2004, we had reported that NOAA had significantly improved risk assessments, security plans, and security control assessments, but needed to improve its C&A process. Our FY 2005 independent

FISMA evaluation found that C&A packages for NOAA's Seattle area LAN and SARSAT were compliant with FISMA, but POES was not. However, even for SARSAT and the Seattle LAN, several important aspects of the C&A process needed to be improved.

NOAA has categorized SARSAT and POES as high-impact systems because a security breach would potentially have severe or catastrophic adverse effects. The certification and accreditation of SARSAT and POES should therefore reflect the highest degree of rigor. The Seattle LAN, as a moderate impact system, would be held to a somewhat lesser standard but a significant degree of due diligence should be manifest in the C&A process.

System Security Plans and Risk Assessments Somewhat Improved

NOAA security plans, which form the basis for certification activities by outlining the security requirements for a system and the controls in place, were improved from those we saw in our FY 2004 review with more accurate accreditation boundaries and better identification of software components and interconnections. But the plans did not accurately depict network components—raising the possibility that certification efforts may not adequately account for such devices. Current interconnection agreements were not in place for POES and SARSAT, which could pose increased risks to agency operations.

Risk assessments for all three systems provided useful information for NOAA system owners to determine appropriate security controls, but we noted some flaws in the assessment methods. Assessed threats and vulnerabilities were either vague or broad generalizations, and analyses at times confused the definitions of some terms. There was no analysis of how controls would mitigate specific adverse events.

We recommended that NOAA require security plans to include a complete and accurate account of all system components and to ensure interconnection agreements are in place. NOAA should use risk assessments to tailor security controls and provide analysis and justifications for resource-intensive changes to the security features of information systems.

Security Control Assessments Insufficient

The POES, SARSAT, and Seattle LAN security control assessments covered only a few of the minimum security controls described in NIST guidance. Generally, the C&A packages did not include specific procedures used to evaluate the controls or complete documentation of the results. In addition, the approach used to select network components for technical control assessments did not provide for complete testing of all operating system variants running on servers, workstations, laptops, routers, and switches.

Describing the System Environment and Interconnections

The security plan provides information that is essential for determining the scope of security control assessments and associating a security deficiency identified during testing with a specific network component. In describing the system environment and interconnections the plan should include the following:

- Detailed topology graphic that depicts system boundary and key components (e.g., perimeter security devices, firewalls, routers, switches, servers).
- Complete listing of hardware and software components.
- Discussion of interconnections with other (both untrusted and trusted) systems, referencing and including copies of memoranda of understandings (MOUs) and other agreements for provision of IT security for the connections.

Source: U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards, June 30, 2005, pages 178–179. Similar requirements were part of the System Security Plan Certification and Accreditation Package Requirements Inspection Checklist, version 2, June 30, 2003

Ineffective Vulnerability Scans

NOAA's use of vulnerability scans to assess the adequacy of security controls was incomplete and ineffective. NOAA's designated scanning tool was unable to evaluate many network components for all three systems. POES scans were successfully completed on only 4 of 14 components residing on its development network, and the operational network was not scanned at all. On the SARSAT system, key components such as firewalls, routers, and switches were not scanned but the system still was accredited. And additional scans of POES and SARSAT done in response to our concerns also were incomplete.

NOAA did not analyze or correct potentially serious vulnerabilities on the Seattle LAN. Two additional scanning tools were used and identified a significant number of vulnerabilities, but the vulnerabilities were not analyzed or corrected prior to the accreditation decision, and they were not identified to the authorizing official.

No Penetration Testing on POES and SARSAT

Penetration testing shows how vulnerable an organization's network is and the level of damage that could result from a system

breach. POES and SARSAT are high-impact systems but, though required, no penetration testing was done.

Our Recommendations

We recommended NOAA undertake comprehensive vulnerability scanning, analyze and document scan results, and plan and implement penetration testing on high-impact systems such as POES and SARSAT. NOAA should comprehensively test all management, operational, and technical controls; perform technical control tests on each operating system variant; and clearly document remaining vulnerabilities for benefit of the authorizing official.

Bureau Response

In its response to our report, NOAA stated that it had completed C&A activities for POES and SARSAT, made immediate revisions to its C&A process after our December 2005 exit conference, and implemented most of our recommended changes. We note that we issued this report because several of the problems we identified in our FY 2005 and previous reviews were evident in the additional five NOAA C&A packages we reviewed early in FY 2006. *(Office of Systems Evaluation: OSE-18019)*

C&A of Contractor IT Resources:

Alternative Approaches

1. Contractor personnel perform the activities, and the system is accredited by a government official as a contractor system.
2. Government personnel and contractor share responsibility for performing the activities, and the system is accredited by a government official as a contractor system.
3. The contractor's IT resources are incorporated into a government system accreditation boundary, and government personnel perform the majority of the activities.

Better Oversight of Contractor Information Security Is Needed

FISMA requires agencies to develop and implement programs to protect government information and information technology systems. With the government's growing reliance on contractors for services, agencies need to perform careful oversight of contractors' information security to avoid misuse of government information or disruption to government IT systems and operations.

In 2002, we reported that Commerce contracts frequently lacked adequate security provisions and we called for IT security clauses to be included.[16] In response to that report, the Department's Office of Acquisition Management and Financial Assistance issued two contract clauses in 2003. Clause 73 requires contractors to comply with the Department's IT security policy and have their IT resources certified and accredited if they connect to a Commerce network[17] or process or store government information. Clause 74 requires contractor personnel to undergo appropriate background screening and IT security awareness training.

To fulfill our charge under FISMA's requirements, we evaluated a judgmental sample of 16 NOAA service contracts to determine whether NOAA is incorporating the two information security clauses into contracts and to evaluate whether their requirements are implemented. Our review also included interviews with managers and staff from NOAA's Office of Acquisition and Grants, Office of the Chief Information Officer, and line offices.

[16] U. S. Department of Commerce, Office of Inspector General. May 2002, *Information Security Requirements Need to Be Included in the Department's Information Technology Service Contracts*. OSE-14788. A subsequent OIG evaluation found that the Department had made progress in incorporating the new IT security clauses into contracts, but provisions for controlling contractor access to Department systems and networks were generally absent, and there was little evidence of contract oversight or of coordination among contracting, technical, and information security personnel. (U.S. Department of Commerce Office of Inspector General, September 2004. *Information Security in Information Technology Security Contracts Is Improving, but Additional Efforts Are Needed*, OSE-16513.)

[17] C&A is required if the connection is to a trusted government network. Trusted networks are the networks inside an organization's network security perimeter, with the exception of virtual private networks (VPNs). These networks are the ones the organization is trying to protect. CISCO Systems Glossary, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4glo.htm (accessed June 13, 2006).

Our Findings

We discovered some problems with aspects of clauses 73 and 74, which contributed to issues we identified at NOAA this year and in a review at USPTO in 2005.[18]

Scope and Content of Clause 73 Should Be Revised

We learned that some NOAA officials and contractors incorrectly interpret Clause 73 to apply only to IT service contracts. Federal information security requirements apply to any organization—including federal assistance recipients or contractors—that has access to government information. Clause 73 is also outdated and contains ambiguous phrases that are interpreted in various ways, which causes some inconsistencies in application.

NOAA Does Not Ensure Contractor IT Resources Are Certified and Accredited

Seven of the 16 contracts in our sample required certification and accreditation, but only 2 had fulfilled the requirement. C&A had not been performed in the other 5 instances because NOAA officials either did not recognize it was required or, if the need was recognized, did not follow through to complete the C&A. The remaining 9 contracts did not require C&A of contractor IT resources because the place of performance was a NOAA facility and the contractors used government IT resources.

Better Guidance Is Needed

It was clear to us that there was some confusion among acquisition and IT security personnel on Clause 73's requirements, the types of contracts it applies to, and the conditions that trigger the need for contractors to certify and accredit their IT resources.

Revising Clause 73 should go a long way toward addressing this issue. But to make sure the clause is properly applied, in addition to updating Clause 73, the Department must develop guidance to assist in resolving four key issues in the acquisition planning stage: whether Clause 73 applies, which Clause 73 requirements apply, the C&A level of effort, and who will perform the C&A.

Key Issues in Performing Contractor Information Security Oversight

1. Application of Clause 73. Contractors need to comply with federal information security policy if they have privileged access to government information, access to government IT resources, or their IT resources are connected to a government trusted network.
2. Clause 73 Requirements. Clause 73 contains two requirements: if the clause applies, the contractor must comply with relevant portions of the DOC IT security policy, but the C&A requirement only applies if contractor IT resources contain government information or provide connection to a government trusted network.
3. C&A Level of Effort. Solicitations need to inform contractors whether their IT resources will be accredited at the low-, moderate-, or high-impact level.
4. C&A Activities. Solicitations need to inform contractors what work is expected to certify and accredit its IT resources.

Clause 74 Requirements Are Not Documented

Contractor personnel generally receive IT security awareness training prior to being granted access to NOAA IT resources. Contracting officer representatives are determining contract risk levels, and contractor personnel are receiving background investigations commensurate with those risk levels as required by Clause 74.

However, we found the risk levels were not documented in contracts or identified in contract files, which made it difficult to determine whether the appropriate risk level had been assigned. In addition, the *Commerce Acquisition Manual* should be updated to reflect the Department's revised IT security policy and the most recent guidance from NIST.

What We Recommended

We recommended the Under Secretary of Commerce for Oceans and Atmosphere and NOAA Administrator primarily address improving the certification and accreditation of contractor IT resources that are either connected to a NOAA trusted network or allow privileged access to government information.

We also recommended the Department's chief financial officer and chief information officer initiate an update of Clause 73 and the *Commerce Acquisition Manual* to be consistent with the Department's IT security policy and NIST standards and guidance. The Department also needs to clarify to which contracts Clause 73 applies and provide additional guidance to assist contracting offi-

[18] Department of Commerce Office of Inspector General, September 2005. *Information Security in Contracts Needs Better Enforcement and Oversight*, OSE-17455.

cers, contracting officer representatives, and IT security officers in implementing information security for contractor IT resources.

Positive Responses from NOAA and the Department

Both NOAA and the Department agreed with our recommendations. The Department's director of acquisition management issued a revised Clause 73 as well as a procurement memorandum that included an information security checklist to assist in determining whether the clause applies to a contract, and if so which provisions apply. The Department also revised the *Commerce Acquisition Manual* section on contract risk designations to be in alignment with the Department's IT security policy. NOAA stated that it will take the appropriate steps to identify contractor IT resources requiring certification and accreditation and implement the C&A process. *(Office of Systems Evaluation: OSE-18028)*

U.S. DEPARTMENT OF COMMERCE

TECHNOLOGY ADMINISTRATION

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 in partnership with the private sector to develop and advocate national policies and initiatives that use technology to build America's economic strength, promote the creation of high-wage jobs, and bring about improvements in our quality of life.

National Institute of Standards and Technology promotes U.S. economic growth by working to develop and apply technology, measurements, and standards. NIST manages four programs: the Advanced Technology Program, the Manufacturing Extension Partnership program, the Baldrige National Quality Program, and NIST Research Laboratories.

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 information collection and dissemination to the public and through information and production services to federal agencies.

Audit Recommends Return of Nearly $800,000 from Cultural Group

In July 2002, the National Institute of Standards and Technology awarded a $1.3 million grant to a not-for-profit organization dedicated to the creation, operation, and administration of cultural and artistic programs. The grant was to pay for real estate and develop programs to create the Puerto Rican Historical, Cultural, and Activities Center (also known as CASA Cultural Puertorriquena), which would include a museum, library, and town hall center to depict the migration of the Puerto Rican people and culture to New York City.

Originally, the NIST award was for a 1-year period beginning July 2002, but the award was amended twice and extended. The first amendment allowed costs incurred prior to the award making the effective start date of the award February 2, 2002. The second amendment extended the award period another year with a new ending date of June 30, 2004. Neither amendment included any additional funds or changes to the award budget. NIST allowed a 90-day closeout period at the end of the award.

Allegations of Wrongdoing

The cultural organization put $500,000 of the award in escrow for a building site and spent more than 2 years trying to purchase the Old Bronx Courthouse to use for the CASA project. The organization finally concluded it did not have sufficient funds to buy the building, the price of which ranged from an initial quote of $1.2 million to $4.8 million. It was considering an alternative site when allegations that the organization had misspent federal funds appeared in New York City newspapers, drawing congressional interest. A New York congressman contacted NIST and asked that the cultural organization be prohibited from spending any more of the grant money.

Since a building had not been acquired, the organization returned the escrowed $500,000 to NIST and submitted a closeout report for the 90-day period July 1 through September 30, 2004, following the end of the award. We audited the organization to determine the financial status of the award, whether the group had complied with all applicable laws and regulations, and whether the expenses charged against the award were allowable.

While the majority of the funding came from NIST and other federal sources over the period of the award, the organization had expended funds for several different projects during this same time period. Only the costs associated with the acquisition of real estate and development programs to create the cultural museum should have been charged to the NIST award but some of the organization's personnel worked on a separate theater renovation project originally funded by the Department of Housing and Urban Development, fund-raising campaigns, and general management along with the CASA project. Expenses were paid based on the money available at the time, not on the source and appropriate use of funds.

The Old Bronx Courthouse was the desired site for a center dedicated to Puerto Rican history, but the price was too high for the cultural organization spearheading the project.

Source: OIG

No Effective Controls

Our audit revealed that the cultural organization did not have effective controls over the NIST funds or adequate procedures to determine allowability of costs for the grant or to allocate expenditures to the four separate cost centers it operated. It filed only four financial status reports, all with the same date, covering the period of August 2002 through March 2004. The organization was unable to explain how the financial status reports had been prepared and could not provide reconciliation of the accounting records or itemized costs.

The organization withdrew a total of $1,290,210 in NIST funds through the award and closeout period. (It drew down the $500,000 for the purchase of real estate during the final month of the award.) The remaining NIST funds drawn down for the award period and closeout period totaled $790,210. During this audit, we repeatedly requested the remaining financial status reports and reconciliation of the group's accounting records to no avail.

The organization also was unable to provide adequate documentation to support the outstanding drawdowns of $790,210 in NIST funds or to substantiate the $607,345 of costs claimed on the financial status reports. We recommended the NIST grants officer recover the full amount of $790,210, which includes questioned costs of $607,345 and excess drawdowns of $182,865. We did not make further recommendations because the award period has expired.

In consideration of the organization's use of its personnel and resources on the CASA project, OIG developed a possible allocation of costs and included it in the appendixes of the audit report. The costs were allocated using OIG's judgment based on discussions with personnel and review of available documentation.

Grantee's Response

In their response to our report, officials of the cultural organization disagreed with the way we allocated costs in our report and said all funds were properly accounted for and all government money was spent for the intended projects. They gave some additional background information, but still did not provide the missing financial status reports or the documentation needed to identify the costs claimed for the award period.

After thoughtful consideration of their objections, our finding that this organization's financial management system was inadequate remains unchanged. We also continue to recommend that NIST disallow the $607,345 in questioned costs and recover the $182,865 in excess drawdowns, a total of $790,210 of funds disbursed. We also have not changed the recommended allocation of costs to CASA that NIST may want to use as an alternative position to disallow a lesser amount of questioned costs since the organization's personnel and resources were used on the CASA project. *(Atlanta Regional Office of Audits: ATL-17744)*

NIST's Advanced Technology Program

As part of its efforts to spur technological development, NIST administers the Advanced Technology Program (ATP) to provide financial assistance through cooperative agreements, with the goal of transferring cutting-edge technology to industrial uses. Between 1990 and September 2004, ATP awarded $2.3 billion to support projects to develop promising, high-risk technologies. Industry has matched this funding with $2.1 billion in cost-sharing.

During this semiannual period, we audited three ATP cooperative agreements to determine whether recipients were complying with federal regulations, NIST ATP requirements, and award terms and conditions. In all, we questioned nearly $500,000 in costs submitted for federal reimbursement. Here are the details of what we found and recommended.

Questioned Costs, Premature Withdrawals Found in California Project

A biotech firm received a 3-year ATP award to develop a genetic engineering technology that would increase commercial production of plant compounds used in vitamins, pharmaceuticals, and

other products. Total estimated costs of the project were $2.8 million, with the federal share capped at $1,987,774 in direct costs.

During the project's first 20 months, the firm reported incurring direct costs of $672,161 but made $800,000 in withdrawals against the award via the government's automated payment system. We identified two problems with this transaction: first, the firm violated ATP program requirements by withdrawing more money than it needed to cover immediate expenses. Second, costs claimed included $195,116 in lab supplies, which the firm calculated as a portion of its company-wide supply costs. This amount is an indirect cost because it was not expended solely on the ATP project. Since indirect costs are not subject to federal reimbursement under this agreement, the firm should have received $477,045 ($672,161-$195,116). We questioned the $195,116 in claimed costs and recommended that NIST recover $322,955 in excess federal funds based on the following calculations:

Direct costs claimed	$672,161
Less questioned costs	195,116
Costs accepted	477,045
Federal funds disbursed	$800,000
Less costs accepted	477,045
Amount due NIST	**$322,955**

We also recommended that NIST take action to ensure that the firm does not withdraw more funds than it needs to cover its immediate costs.

Finally, we found that the firm did not have written standards for employee conduct or written procedures for minimizing the time between receipt and disbursement of federal funds, making procurements with award dollars, and determining whether costs are allowable. We recommended that NIST direct the firm to develop and enforce the required written standards and procedures. *(Denver Regional Office of Audits: DEN-17931)*

Colorado Firm Bills for Nonproject Expenses, Miscalculates Federal Share

A Boulder firm is using ATP funds to develop laser technology for measuring optical frequencies far faster and more accurately than is currently possible. The technology has potential application and benefits for a range of U.S. industries—optical communications, aerospace, semiconductor manufacturing, and medical diagnostics, to name a few. The 2-year project has total estimated costs of $2,199,076, with the federal share not to exceed $2 million (93.8 percent).

From June 2004 through September 2005, the firm reported costs of $1,302,263 and received $1,273,369 in reimbursement. Our interim audit questioned $12,466 in costs claimed, consisting of $8,966 for equipment purchased outside of the award period and $3,500 in unallowable relocation expenses. The firm also had calculated reimbursement at a higher rate than allowed for by the award (98.7 percent versus 93.8 percent) and as a result received excess reimbursement totaling $63,539, which includes the questioned amount. Finally, we found that the company had not labeled equipment purchased with federal funds to indicate government ownership.

We recommended that NIST disallow the questioned costs, recover $63,539 in excess reimbursement, and direct the recipient to properly tag all project-related equipment purchased with federal funds. *(Denver Regional Office of Audits: DEN-17832)*

Software Costs at Issue in California/Nevada Joint Venture

In April 2004, a California company and a Nevada firm received $1.5 million in ATP funding to develop a prototype diesel engine built on a thermal technology that—if successful—promised huge gains in fuel efficiency along with reduced emissions. The 2-year award capped federal contributions to the California firm at 42.02 percent of allowable costs. The federal share to the Nevada firm was capped at 36.53 percent. We audited costs claimed by the companies during the project's initial 20 months (May 2004 through December 2005).

The California firm incurred $789,271 in costs and received $374,377 in federal reimbursement. We questioned $84,424 in unsupported costs for, among other things, software that had been developed prior to the award, as well as tools and equipment that had been previously purchased. We recommended that NIST disallow the questioned costs and recover the federal share of $78,200.

The Nevada firm submitted costs of $393,210 and received $149,943 in reimbursement. We questioned $130,181, largely in unsupported software development expenditures, and recommended that NIST disallow the full amount as well as recover $53,859 in excess federal disbursements. *(Denver Regional Office of Audits: DEN-17933-6-0001 and 0002)*

Audits Unresolved for More Than 6 Months

Massachusetts MEP

We are continuing to work with NIST officials toward resolution of an MEP cooperative agreement, which we reported on in our September 2004 *Semiannual Report* (page 37) as being unresolved for more than 6 months. Our audit had recommended that NIST disallow questioned costs of $8,177,606, recover the federal share of $1,599,349, and require the recipient to implement improvements to its financial reporting system. In its audit resolution proposal, NIST disallowed $715,097 and reinstated $7,462,509 in costs questioned in the audit report. In July 2004, after detailed analyses of NIST's audit resolution proposal and other documents provided by NIST and the recipient, we advised NIST that we concurred with its decision to disallow $715,097, but did not concur with reinstatement of the remaining $7,462,509. OIG is reviewing a revised audit resolution proposal that NIST submitted in June 2005.

Computer Aided Surgery Inc., New York

An OIG audit of this NIST cooperative agreement (see September 2004 issue, page 35, and March 2005 issue, page 33 — ATL-16095) questioned costs totaling $547,426 in inappropriately charged rent, utilities, and certain salary, fringe benefit, and other expenses, because these costs were unallowable, in excess of budgetary limits, or incorrectly categorized. This audit remains unresolved because we have postponed NIST's submission of an audit resolution proposal.

FastVDO LLC, Maryland

A financial assistance audit of this NIST cooperative agreement (see March 2006 issue, page 35, DEN-17410) recommended that NIST disallow $51,838 in questioned costs, recover excess federal disbursements of $29,409, and ensure the recipient, among other things, (1) implements an adequate method for capturing time directly spent on the ATP project, (2) bills only for that time, (3) develops written financial management procedures, and (4) tracks and inventories grant-funded purchases as required by federal regulations and ATP program terms. This audit remains unresolved because we have postponed NIST's submission of an audit resolution proposal.

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 tools to maximize U.S. competitiveness.

Goal 2: Foster science and technological leadership by protecting intellectual property, enhancing technical standards, and advancing measurement science.

Goal 3: Observe, protect, and manage the Earth's resources to promote environmental stewardship.

The Department has also established a Management Integration Goal that is equally important to all bureaus: **Achieve organizational and management excellence**.

Commerce Implemented Reasonable Precautions for Special Hurricane Procurements

In the aftermath of the 2005 hurricanes Katrina and Rita, PCIE's Homeland Security Working Group coordinated the inspectors general reviews of post-hurricane spending and examined relief efforts provided by the federal government because of expressed concerns about the potential for fraud and waste in the massive effort. As part of the project, we surveyed Department of Commerce contracts and financial assistance awards made in the wake of hurricanes Katrina and Rita to determine whether the Department had taken reasonable steps to reduce the potential for fraud, waste, and abuse. Although the hurricanes represented significant catastrophic events, we found that, on the contracts and financial assistance awards we examined, the Department implemented reasonable precautions to protect the interests of the government and ensure funds were handled appropriately.

NIST awarded one $300,000 contract to a California-based nonprofit corporation to conduct a field study of damage caused by the hurricanes to major buildings, residential construction, and different types of infrastructure, and to report on the findings and any recommendations for more detailed studies. NIST cited an unusual and compelling urgency for the services to award the contract noncompetitively and stated the proposed contractor was the only responsible source that could meet the government's needs.

NOAA made 668 individual hurricane-related purchases, with obligations totaling about $6.56 million. Cumulatively, some 608 of the purchases accounted for less than $300,000 of NOAA's total. The remaining 60 purchases totaled about $6.27 million.

Procurement Personnel Dispatched to Pascagoula, Mississippi

Most of NOAA's 60 largest procurements involved emergency response and recovery operations at a severely damaged NOAA facility in Pascagoula, Mississippi. NOAA facilities in Miami, Florida, and at Stennis Space Center in Mississippi also suffered damage from the hurricane. NOAA's director of acquisitions and grants designated NOAA's Central Region Acquisition Division in Kansas City, Missouri, as the lead office responsible for quickly restoring those operations. The director of the Central Region Acquisition Division and a NOAA project engineer were deployed from Kansas City to Pascagoula immediately after the hurricane to provide on-site procurement support and oversee contractors.

Katrina's storm surge flooded part of NOAA's Pascagoula, Mississippi, facility. The high water mark is visible on the center wall—about 4 feet.

Source: OIG

Hurricane flooding wrecked the library in NOAA's National Marine Fisheries Service offices in Pascagoula, Mississippi, destroying valuable research materials.

Source: OIG

On September 7, 2005, the Central Region Acquisition Division director made a class action determination that full and open competition was not required for supplies and services in response to Hurricane Katrina because NOAA's need for those supplies and services was of an unusual and compelling nature and the government would be seriously injured unless NOAA was permitted to limit the number of sources from which it solicited quotes, bids, or proposals. Such class action determinations are permitted by Section 6.303-1(c) of the Federal Acquisition Regulation.

The NOAA contracting officer determined that NOAA's needs would best be served by awarding the cleanup and repair of the Pascagoula facility to a construction contractor who had been working on renovation and expansion prior to the hurricane, rather than delaying the cleanup while locating another contractor. We examined the contracting office's written justification to award noncompetitively and the terms of the contract. We also obtained a written certification from the NOAA project engineer deployed to Pascagoula stating that the prices paid to the government were fair and reasonable.

In addition to facility cleanup and repair, managers of the damaged Pascagoula offices and laboratories also teamed with the contracting officer and project engineer from Kansas City to buy modular buildings (trailers) to serve as temporary work space, replacement office and laboratory equipment and supplies, and replacement vehicles. We reviewed a sample of the contracts entered into and found that most were awarded competitively, under normal Commerce procedures. We also examined receiving records and toured the Pascagoula facility to observe the ongoing repair work and confirm receipt of items purchased.

These outdoor freezers at NOAA's National Seafood Inspection Laboratory in Pascagoula, Mississippi, were completely submerged by Hurricane Katrina's storm surge.

Source: OIG

Finally, we examined specific instances in which NOAA used emergency expanded procurement authorities granted in the aftermath of Hurricane Katrina. Federal law allows agencies to increase certain procurement thresholds and limitations to support a national emergency and eight NOAA contracting officers received emergency expanded procurement authorities. NOAA contracting officers utilized increased authorities for only nine procurements. Five involved the expanded simplified acquisition authority at the hurricane-damaged Pascagoula, Mississippi, facility to lease temporary work space, purchase generators to provide electrical power, and purchase replacement laboratory supplies and equipment. The largest of the five simplified acquisitions totaled $140,000. The remaining uses of increased purchase authorities involved three purchases of equipment, ranging in amount from a little more than $10,000 to just under $14,000, and a waiver of a small business set-aside for a $15,000 contract with a nonprofit marine sanctuary foundation.

Based on our limited review, we believe that the Department implemented reasonable precautions, given the circumstances of a significant catastrophic event, to protect the interests of the government and award contracts in a timely manner.

Financial Assistance Awards Were Reasonable and Handled Properly

Three Commerce bureaus made a total of six financial assistance awards, involving about $9.42 million in federal funding, in the aftermath of hurricanes Katrina and Rita:

EDA awarded four grants totaling $8,840,000 to the states of Louisiana ($4 million), Mississippi ($4 million), and Alabama ($450,000 and $390,000) for economic recovery planning and technical assistance in the aftermath of Hurricane Katrina.

MBDA awarded a $300,000 cooperative agreement amendment to the Houston Minority Business Development Center for supplemental funding to provide business development services to minority-owned businesses affected by Hurricane Katrina in the state of Louisiana and to displaced minority firms from Louisiana relocated in Texas. There was no nonfederal matching share requirement for the amendment.

NTIA awarded a grant with a federal share of $283,320 to the Louisiana Educational Television Authority, under the Public Telecommunications Facility Program, for emergency replacement of transmission equipment. The grant required a nonfederal match of $94,440, bringing the total estimated project cost to $377,760.

After reviewing the EDA, MBDA, and NTIA award documents and regulations and discussing the awards with agency officials, we believe the Department actions to award the grants were reasonable. *(Denver Regional Office of Audits: DEN-17829)*

Framing and electrical wiring repairs were required after Hurricane Katrina damaged NOAA's National Marine Fisheries Service offices in Pascagoula, Mississippi.

Source: OIG

Preaward Financial Assistance Screening

As part of our ongoing emphasis on prevention of fraud, waste, and abuse, we continue to work with the Office of Acquisition Management, NOAA and NIST grant offices, and EDA program offices to screen the Department's proposed grants and cooperative agreements before they are awarded. 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.

On January 1, 2004, we implemented new policies and procedures for our preaward screening process. OIG and the Department determined that there are several categories of recipients for whom the costs and administrative burden of the screening process may well outweigh the government's risk of financial loss. Our new policies exempt from review, recipients who (1) receive awards in amounts of $100,000 or less; (2) have received financial assistance from the Department for 3 or more consecutive years without any adverse program or audit findings; or (3) are units of a state or local government.

During this period we screened 192 proposed awards. For 33 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 22 awards and established special award conditions for 11. *(Office of Audits)*

Preaward Screening Results

Award		
Results	**Number**	**Amount**
Awards delayed to resolve concerns	22	$25,884,555
Special award conditions established	11	$13,235,825

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 231 audit reports during this semiannual period to determine whether they contained any audit findings related to Department programs. For 152 of these reports, the Department acts as oversight agency and monitors the audited entity's compliance with the OMB Circular A-133 or NIST's program-specific reporting requirements. The other 79 reports are from entities for which other federal agencies have oversight responsibility. We identified 28 reports with findings related to the Department of Commerce.

Report Category	OMB A-133 Audits	ATP Program-Specifics Audits	Total
Pending (April 1, 2006)	33	118	151
Received	142	34	176
Examined	119	112	231
Pending (September 30, 2006)	56	40	96

The following table shows a breakdown by bureau of more than $660 million in Commerce funds audited.

Bureau	Funds
EDA	$ 41,898,642
NIST*	176,036,009
NOAA	39,208,751
NTIA	362,644
Multiagency	402,954,880
Agency not identified	22,429
Total	$660,483,355

* Includes $169,942,322 in ATP program-specific audits.

We identified a total of $3,643,795 in federal questioned costs and $2,846,452 in funds to be put to better use. 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 28 reports with Commerce findings are listed in Appendix B-1. (*Atlanta and Denver Regional Offices of Audits*)

OFFICE OF INSPECTOR GENERAL

Office of Investigations

The mission of the **Office of Inspector General** is to promote economy, efficiency, and effectiveness and detect and prevent waste, fraud, abuse, and mismanagement in the programs and operations of the U.S. Department of Commerce. Through its audits, inspections, performance evaluations, and investigations, OIG proposes innovative ideas and constructive solutions that lead to positive changes for the Department. By providing timely, useful, and reliable information and advice to departmental officials, the administration, and Congress, OIG's work helps improve Commerce management and operations as well as its delivery of services to the public.

During this semiannual period, the Office of Investigations maintained its focus on areas within the traditional IG investigative portfolio—fraud, waste, and abuse in Commerce programs and operations—while expanding its reach to combat other forms of internal and external corruption that negatively impact the Department, the federal government, and taxpayers. Notable work conducted over the past 6 months includes investigation of a massive international telemarketing scam and a major immigration fraud ring. We also achieved impressive results in a diverse array of cases involving grant fraud, bribery, theft, and criminal misuse of government computer resources in connection with child pornography. The investigations highlighted below are representative of our recent accomplishments in these and other areas of critical concern.

Investigation of International Telemarketing Fraud Yields Multiple Arrests, Indictments, and Convictions

For the past 3 years, OIG has been investigating a major telemarketing fraud scheme based in Costa Rica that was perpetrated by callers identifying themselves as employees of the Commerce Department and other federal agencies. The callers told victims in the United States that they were winners in a national lottery sanctioned by the Department and that they had won sweepstakes prizes ranging in value from $450,000 to more than $4 million. Victims were then instructed to use commercial wire transfer services to send payments of $1,500 to $4,500 to Costa Rica, purportedly for insurance and customs fees that were required to retrieve their winnings. Many victims were persuaded to send multiple payments to the telemarketers—some individuals transferred more than $200,000. Total identified losses to U.S. residents exceed $30 million to date.

The investigation is being conducted in conjunction with the U.S. Postal Inspection Service, the Bureau of Immigration and Customs Enforcement of the Department of Homeland Security, and several foreign law enforcement agencies, and is an integral part of the Department of Justice's Operation Global Con, the largest international mass marketing fraud investigation of its kind. To date, Operation Global Con investigations have developed evidence of several massive international confidence schemes that have defrauded nearly 3 million victims of more than $1 billion.

In May 2006, OIG spearheaded the simultaneous execution of 17 search warrants in the United States and Costa Rica, targeting telemarketing call centers and the residences of several principal participants in the scheme. The search operation required coordination among about 200 U.S. and Costa Rican law enforcement officers, 17 Costa Rican judges, and 24 Costa Rican prosecutors. It resulted in the arrest and subsequent indictment of 18 American and Canadian citizens located in Costa Rica, Panama, and the United States who were identified as owners or employees of the call centers in Costa Rica. We also seized $400,000 in cash, multiple weapons, and a variety of equipment used to facilitate the scheme, including numerous Voice over Internet Protocol telecommunications devices, which were employed to disguise the telemarketers' true location by displaying area codes indicating that the calls originated in the United States.

The defendants all were indicted on multiple counts of conspiracy, wire fraud, and money laundering in the Western District of North Carolina. Since that time, indictments or criminal informations have been filed against an additional eight participants in the scheme, including five Costa Rican nationals. Two of the defendants have already pleaded guilty to conspiracy to commit wire fraud.

In addition, on August 2, 2006, a Costa Rican attorney previously indicted for his part in the telemarketing scheme (see March 2006 *Semiannual Report*, page 48) was convicted in U.S. District Court for the Southern District of Florida on two counts of money laundering. His sentencing was scheduled for November 2006. (*Atlanta Field Office*)

NOAA Employee Sentenced to 15 Years on Child Pornography Conviction

Our March 2006 *Semiannual Report* (page 51) reported the indictment and arrest of a longtime NOAA employee for sexual exploitation of children and possession of child pornography following an OIG investigation that found he had been using government and personal computers to download sexually explicit images of children for at least a decade. An extensive forensic examination of the employee's home and office computers revealed more than a million pornographic images of children, and a search of his residence uncovered evidence that he was personally involved in the production of child pornography. Thousands of slides and photographic negatives discovered during the search disclosed images of a young child involved in sexual activity with an adult male resembling the defendant. OIG investigators identified and interviewed the now adult victim, who confirmed that the defendant had engaged in and photographed sexual relations with her on an ongoing basis from the time she was about 8 years old until she was 14.

OIG special agents store seized evidence.

Source: OIG

Rather than face arrest, the defendant fled the country after his indictment, traveling from his brother's home in California to various locations in Canada and Europe. By employing sophisticated investigative tracking techniques and an extensive network of law enforcement agencies in the United States and abroad, OIG was able to quickly trace him from Vancouver to Prague, and finally to Italy. We had previously made contact with the national television program *America's Most Wanted,* which aired a segment on the investigation on January 21, 2006. Within 48 hours of the broadcast, the defendant contacted the American Embassy in Rome and made arrangements to surrender.

In May 2006, the defendant pleaded guilty to possession and production of child pornography. On August 30, 2006, he was sentenced in U.S. District Court for the District of Maryland to 15 years in prison followed by 3 years' supervised probation, and ordered to liquidate his federal thrift savings account and pay all proceeds to the victim identified during our investigation as restitution for his crimes.

The defendant's brother still faces criminal charges in the Eastern District of California for helping the defendant evade arrest by failing to disclose his whereabouts to OIG investigators and warning him that we had traced his movements to Canada. *(Computer Crimes Unit)*

Government Reaps $2 Million Settlement in *Qui Tam* Lawsuit

A manufacturer of water storage tanks used in federally funded development projects agreed to a $2 million settlement in order to resolve claims that the tanks were not constructed in accordance with contract specifications. For a period of about 10 years, the company supplied steel water storage tanks for projects funded under grant programs administered by EDA and the Departments of Agriculture and Housing and Urban Development. A *qui tam* action filed in the Southern District of Indiana by a former employee of the company alleged that the welds used by the company to construct certain tanks did not meet contract specifications and that the use of a less expensive and potentially less effective welding technique rendered the tanks less structurally sound than required. It was also alleged that the company conspired with an engineering firm to generate false testing records to show that the tanks it manufactured met contract specifications.

In April 2006, following a joint investigation conducted by the Commerce, Agriculture, and HUD OIGs, the company agreed to a settlement that provides a payment of $1.75 million to the government over an 18-month period, along with extended warranties valued at $250,000, under which the company agrees to repair at its sole expense any failures, leaks, or degradation resulting from substandard welding. Under the terms of the agreement, the former employee who initiated the action will receive $400,000 of the settlement proceeds. The company will also pay him $50,000 to cover his legal costs. (*Silver Spring Resident Office*)

Former Census Employee Indicted for Workers' Compensation Fraud

On July 11, 2006, a former Census field representative was indicted in U.S. District Court for the Northern District of Georgia on five counts of making false statements to collect federal work-

ers' compensation benefits for work-related injuries sustained in a 1994 automobile accident. An OIG investigation disclosed that the former employee failed to report more than $40,000 in earnings from a retail job and the operation of a show dog kennel when filing annual certifications with the Department of Labor between 2001 and 2005. As a result of her false reporting, she fraudulently received about $89,000 in workers' compensation benefits. The defendant was released on bond pending further proceedings. A trial date has not yet been set. *(Atlanta Field Office)*

Sentencing in Patent Office Bribery Scheme

We previously reported the conviction of a draftsman at USPTO for his participation in a bribery scheme initiated by his supervisor, who solicited payment from patent applicants in exchange for drafting work performed by her staff. (See March 2006 *Semiannual Report*, page 49.) In May 2006, the defendant was sentenced in U.S. District Court for the Eastern District of Virginia to 1 year probation, a $1,000 fine, and $100 in restitution. In August 2006, a second employee implicated in the scheme agreed to enter the Department of Justice's Pretrial Diversion Program in order to resolve the charges against him. Under the terms of the agreement, all pending charges will be dismissed upon his successful completion of a 6-month period of supervision under the program, which will include 50 hours of approved community service. (*Alexandria Resident Office)*

NOAA Employee and Spouse Convicted for Use of Government Gas Cards

In May 2006, a NOAA employee and her husband were convicted of theft from the government after a joint investigation with the General Services Administration OIG revealed that the couple had on multiple occasions used GSA automotive fleet credit cards assigned to NOAA to purchase gasoline for their personal vehicles and the vehicles of others. On August 2, 2006, both defendants were sentenced in U.S. District Court for the District of Maryland. The employee was sentenced to 1 year probation, 50 hours of community service, and $448 in restitution. Her husband received a sentence of 2 years' probation, 90 days in a halfway house, and restitution of $448. Based on her conviction, NOAA has proposed the employee's removal from federal service. *(Silver Spring Resident Office)*

Commerce Employee Arrested for Role in Immigration Fraud Ring

A senior patent examiner was one of 19 individuals arrested on September 7, 2006, in connection with an immigration fraud scheme operating in Maryland, Northern Virginia, and the District of Columbia, which entailed the orchestration of sham marriages between American citizens and foreign nationals seeking legal immigration status in the United States. The arrests were the result of a 3-year task force investigation involving Commerce OIG, the Department of Homeland Security's Immigration and Customs Enforcement branch, the State Department OIG, and several other federal, state and local law enforcement agencies.

Nine of those arrested—including the USPTO employee—are charged with facilitating the scheme by arranging fraudulent marriages for a fee. The other 10 are foreign nationals who entered into sham marriages in order to gain immigration benefits and avoid deportation from the United States. Arrest warrants have also been issued for 3 American citizens who were paid to marry aliens as part of the scheme. Charges have been filed against the defendants in the Eastern District of Virginia for multiple violations of federal law, including immigration fraud, conspiracy to defraud the United States, and filing false statements.

The investigation was initiated after a clerk at the Arlington County Courthouse observed that the same individual was escorting groups of citizen/noncitizen couples to apply for marriage licenses on a

weekly basis and often returned with the couples a short time later to assist them in filing for divorce. (*Alexandria Resident Office)*

Subcontractor on EDA Project Sentenced for His Role in Bribery Scheme

In our March 2006 *Semiannual Report* (page 48), we reported the conviction of a construction company owner for his role in an extortion scheme run by a Philadelphia city official, who accepted bribes to issue minority business certificates for use in bidding on federally-funded construction projects, including several funded by EDA. On August 29, 2006, the defendant was sentenced in U.S. District Court for the Eastern District of Pennsylvania to 5 years' probation and a $6,000 fine and was ordered to pay restitution in the amount of $31,852. (*Alexandria Resident Office)*

Former NOAA Employee Convicted of Theft for Time and Attendance Fraud

A former NOAA employee was convicted of theft in the District Court of Maryland for Montgomery County after an OIG investigation found that he had manipulated the office's time and attendance database and altered manual timekeeping records to obtain more than $11,000 in unearned salary over an 18-month period. In June 2006, he was sentenced to 12 months' supervised probation, fined $400, and ordered to make full restitution to the agency. The employee retired from federal service shortly after his arrest. *(Washington Field Office)*

Additional Convictions and Arrest for T&A Fraud at USPTO

Our March 2006 *Semiannual Report* (page 50) reported the arrests of two USPTO employees, which resulted from OIG investigative findings that the former patent examiners had embezzled a total of nearly $6,000 from the agency by falsely claiming pay for hours not worked.

On May 5, 2006, one of the defendants was convicted of theft in the Circuit Court of the City of Alexandria, Virginia. She was sentenced to 30 days' incarceration and ordered to pay $1,444 in restitution. The second defendant was indicted on felony theft charges in June 2006 for defrauding USPTO of approximately $4,470 in salary payments. After pleading guilty to the charges in August 2006, she was sentenced in Alexandria Circuit Court on September 21, 2006, to 2 years' probation and 50 hours of community service, and ordered to make full restitution to the government. Both employees had resigned from the agency prior to arrest.

Another former patent examiner was arrested by OIG on July 10, 2006, and charged in Alexandria Circuit Court with embezzling more than $21,000 from USPTO between June 2005 and January 2006 by submitting falsified time and attendance records. The defendant has been released on her own recognizance pending further proceedings. *(Alexandria Resident Office)*

OIG Recovers Missing Weather Service Equipment

Early this year, OIG received information that meteorological equipment belonging to the National Weather Service was being offered for sale on eBay. We identified the equipment as part of a shipment of 50 radiosondes that was either lost or stolen while in transit from the National Logistics Supply Center in Kansas City, Missouri, to a local weather forecast office. Radiosondes are balloon-borne instruments used to transmit meteorological measurements—such as wind speed and barometric pressure—from the upper atmosphere to ground stations. OIG investigators located the eBay seller, who had purchased 30 of the missing instruments at an auction in North Carolina. We seized the 23 radiosondes still in his possession, as well as his customer list, and subsequently recovered an additional 6 units from purchasers. The investigation is continuing. *(Atlanta Field Office)*

Other OIG Activities

Commerce Inspector General Testifies Before House Science Committee on NPOESS

On May 11, Inspector General Johnnie E. Frazier testified before the U.S. House of Representatives Committee on Science about findings in an OIG report on cost overruns and schedule delays of the triagency National Polar-orbiting Operational Environmental Satellite System (NPOESS) weather satellite program.

Frazier told the committee that OIG's review uncovered two overarching management and contract weaknesses that resulted in unchecked cost and schedule overruns in the NPOESS program. First, the executive committee of the triagency program, comprised of top NOAA, Department of Defense, and NASA officials, never challenged optimistic assessments of the impact of technological problems. Second, the contractor received excessive award fees despite problems.

"Inadequate management oversight, in effect, postponed critical evaluations and decisions needed to replan the program's faltering elements and contain cost and schedule overruns," Frazier said. "Time and money were thus wasted as NPOESS problems continued unchecked."

Frazier said OIG's audit questioned why fees were paid for unsatisfactory performance and the contractor was allowed to roll over unearned fees. "The intimate connection between the director's professional reputation and the success of both the program and the contractor could affect his objectivity as fee determining official in setting award amounts," Frazier added.

Vice Admiral Conrad C. Lautenbacher (ret.), administrator of NOAA, also testified before the committee, saying NPOESS had a history of budget and technical problems but that actions were being taken to address them. He said the NOAA employee who previously directed the project had resigned, and the prime contractor had changed the personnel on the project. Lautenbacher added that an Air Force Brigadier General had stepped in as director, raising "concerns about whether NOAA and NASA priorities will still receive adequate attention."

Rep. Sherwood L. Boehlert, chairman of the Committee on Science, said NPOESS' success is vital to the nation but the program was not succeeding and needed to get on track.

"What I want to hear clearly is an admission that NOAA — and that means NOAA's leadership right up to the top — made mistakes, can identify those mistakes, and has plans to fix those mistakes," Boehlert said. "I am not suggesting that anyone was not trying to do their best in running the NPOESS program. But I am suggesting that previous management procedures clearly were not successful."

Vernon J. Ehlers, chairman of the Subcommittee on Environment, Technology and Standards, said he had been assured in 2004 that problems were being solved. "And here we are again, now billions over budget, with delays long enough that we are facing large potential gaps in life-saving satellite data. This cannot continue," Ehlers said. "We must make sure that we have the satellites we need when we need them, and effective management of the procurement and acquisition process is essential to meeting this goal."

Commerce OIG has named managing the environmental satellite program as one of the Department's top management challenges. "I am pleased to note that in his response to our report, Deputy Secretary (David) Sampson stated that both he and Secretary (Carlos) Gutierrez are fully committed to providing strong oversight and management of NPOESS," Frazier added.

On May 22, the House Science Committee introduced HR 5450, the National Oceanic and Atmospheric Administration Act, which among other things, creates the position of deputy assistant secretary for science and education. The bill also requires NOAA to notify Congress and the public if it plans to close or transfer a NOAA facility, and if it starts a new satellite program, or encounters problems or makes major changes to an existing satellite program. The bill passed in the House of Representatives on September 21, 2006, and was referred to the Senate Committee on Commerce, Science, and Transportation.

Commerce Inspector General Johnnie E. Frazier (left) testified before the House Science Committee about the environmental satellite program's schedule delays and cost overruns on May 11. Vice Admiral Conrad C. Lautenbacher (ret.), administrator of NOAA, (right) also testified before the committee.

Source: House Science Committee

On June 8, 2006, the House Committee on Science held a hearing on the results of the statutorily required Nunn-McCurdy review. The Nunn-McCurdy provision of the National Defense Authorization Act requires that any DoD-funded program that is more than 25 percent over budget be reviewed to see if it should be continued and how.

The review, which was carried out under the auspices of DoD by all three NPOESS agencies, determined that the program should be continued with fewer satellites of lesser capability. The agencies maintain that no additional funds beyond what is projected will be needed until FY 2010.

(A summary of the OIG report appears on page 29. The full report, OIG-17794: *Poor Management Oversight and Ineffective Incentives Leave NPOESS Program Well Over Budget and Behind Schedule*, can be viewed at www.oig.doc.gov/oig/reports/audit_inspection_and_evaluation_reports/index.html.)

OIG Investigators Honored

Several staff members in the Office of Investigations were recognized during this semiannual period by groups outside the Department.

A criminal investigator in our Atlanta Field Office was named *Special Agent of the Year* by the Southeast Region of Inspectors General Council as a result of his exceptional work in the telemarketing fraud investigation detailed on page 47.

The special agent-in-charge of our Computer Crimes Unit received a Certificate of Honorable Mention from the National Center for Missing and Exploited Children (NCMEC) for identifying a new victim for inclusion in NCMEC's national database of missing and exploited children while investigating the case reported on page 48.

Finally, during this period, a criminal investigator in our Denver Resident Office received the *Guardian of Justice* award from the U.S. Attorney's Office for the District of Kansas, as well as a Distinguished Achievement Award from the Colorado chapter of the Association of Certified Fraud Examiners. Both awards honored his work in connection with a successful fraud and money laundering investigation, which he conducted while serving in his previous position with the Office of Inspector General at the Department of Health and Human Services.

TABLES AND STATISTICS

Statistical Overview

TABLES	PAGE
1. Investigative Statistical Highlights for this Period	53
2. Audit Resolution Follow-Up	54
3. Audit and Inspection Statistical Highlights for this Period	54
4. Audits with Questioned Costs	54
5. Audits with Recommendations that Funds Be Put to Better Use	55
APPENDIXES	
A. Report Types this Period	56
A-1. Performance Audits	56
A-2. Financial Assistance Audits	57
A-3. Inspections and Systems Evaluations	58
B. Processed Audit Reports	59
B-1. Processed Reports with Audit Findings	60

Table 1. Investigative Statistical Highlights for this Period

Investigative Activities	
Arrests	26
Indictments and informations	32
Convictions	10
Personnel actions	6
Fines, restitutions, judgments, and other civil and administrative recoveries	$2,112,812
Allegations Processed	
Accepted for investigation	47
Referred to operating units	14
Evaluated but not accepted for investigation or referral	26
Total	87

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, 2006) for which no management decision had been made by the end of the period (September 30, 2006). Eight audit reports remain unresolved for this reporting period (see pages 23, 24, and 42).

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.

Table 2. Audit Resolution Follow-Up

Report Category	Modifications	Appeals
Actions pending (April 1, 2006)	1	10
Submissions	2	2
Decisions	3	5
Actions pending (September 30, 2006)	0	7

Table 3. Audit and Inspection Statistical Highlights for this Period

Questioned costs	$ 4,145,894*
Value of audit recommendations that funds be put to better use	3,495,106
Value of audit recommendations agreed to by management	1,704,308
Value of inspection recommendations that funds be put to better use	N/A

*This number includes costs questioned bt state and local government auditors or independent public accountants.

Table 4. 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	19	$26,943,444	$ 5,425,575
B. Reports issued during the reporting period	30	4,145,894	214,733
Total reports (A+B) requiring a management decision during the period[1]	49	31,089,338	5,640,308
C. Reports for which a management decision was made during the reporting period[2]	16	4,471,814	1,541,220
i. Value of disallowed costs		809,741	538,100
ii. Value of costs not disallowed		3,802,657	1,003,120
D. Reports for which no management decision had been made by the end of the reporting period	33	26,617,524	4,099,088

NOTES:

[1] Nine audit reports included in this table are also included among reports with recommendations that funds be but to better use (see table 5). However, the dollar amounts do not overlap.

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

Table 5. 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	7	$ 2,975,478
B. Reports issued during the reporting period	10	3,495,106
Total reports (A+B) requiring a management decision during the reporting period[1]	17	6,470,584
C. Reports for which a management decision was made during the reporting period[2]	9	3,040,360
i. Value of recommendations agreed to by management		894,567
ii. Value of recommendations not agreed to by management		2,202,301
D. Reports for which no management decision had been made by the end of the reporting period	8	3,430,224

[1]Nine audit reports included in this table are also included in the reports with questioned cost (see table 4). 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.

Definitions of Terms Used in the Tables

Questioned cost: a cost 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: an OIG recommendation 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.

Appendix A. Report Types this Period

Type	Number of Reports	Appendix Number
Performance audits	2	A-1
Financial assistance audits	8	A-2
Inspections and systems evaluations	6	A-3
Total	**16**	

Appendix A-1. Performance Audits

Report Title	Report Number	Date Issued	Funds to Be Put to Better Use
National Oceanic and Atmospheric Administration			
Poor Management Oversight and Ineffective Incentives Leave NPOESS Program Well Over Budget and Behind Schedule	OIG-17794-6-0001	05/08/06	
Office of the Secretary			
A Survey of Hurricane Katrina and Hurricane Rita Contracts and Grants	DEN-17829-6-0001	07/20/06	

Appendix A-2. Financial Assistance Audits

Report Title	Report Number	Date Issued	Value of Funds to Be Put to Better Use	Federal Amount Questioned	Federal Amount Unsupported
Economic Development Administration					
City of Clovis, CA	STL-17578-6-0001	07/31/06			
Shorebank Neighborhood Institute, IL	DEN-17932-6-0001	09/27/06	$ 648,654	$ 81,568	
City of Dinuba, CA	STL-17579-6-0001	09/29/06			
City of Greenfield and County of Monterey, CA	STL-17580-6-0001	09/30/06		130,692	$ 24,958
National Institute of Standards and Technology					
Precision Photonics Corporation, CO	DEN-17832-6-0001	04/14/06		11,693	
ReJen Company, NV	DEN-17933-6-0001	09/14/06		47,555	47,555
Alvin Lowi & Associates, Inc., CA	DEN-17933-6-0002	09/15/06		35,475	35,475
Sangamo BioSciences, Inc., CA	DEN-17931-6-0001	09/15/06		195,116	

Appendix A-3. Inspections and System Evaluations

Agency	Report Title	Report Number	Date Issued	Funds to Be Put to Better Use
Census				
	Enumerating Group Quarters Continues to Pose Challenges	IPE-18046	09/29/06	—
International Trade Administration				
	Commercial Service Operations in Argentina and Uruguay Are Mostly Sound but Financial Processes Need Attention	IPE-18111	09/25/06	—
	Commerce Should Ensure that Travelers to China Receive Counterintelligence Briefings	IPE-17954	07/25/06	—
National Oceanic and Atmospheric Administration				
	SARSAT's E-Authentication Controls Do Not Provide Adequate Assurance of Users' Identities	OSE-18020	09/15/06	—
	Additional Steps Are Necessary to Provide Better Oversight of Contractor Information	OSE-18028	09/29/06	—
	Progress Being Made in Certification and Accreditation Process, but Authorizing Officials Still Lack Adequate Decision-making Information	OSE-18019	09/19/06	—

Appendix B. Processed Audit Reports

The Office of Inspector General reviewed and accepted 231 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 non-financial recommendations are listed in Appendix B-1.

Agency	Audits
Economic Development Administration	40
National Institute of Standards and Technology*	118
National Oceanic and Atmospheric Administration	20
National Telecommunications and Information Administration	3
Multiagency	48
Agency not identified	2
Total	231

*Includes 112 ATP program-specific audits.

Appendix B 1. Processed Reports with Audit Findings

Report Title	Report Number	Date Issued	Value of Funds to Be Put to Better Use	Federal Amount Questioned	Federal Amount Unsupported
Economic Development Administration					
Cumbres & Toltec Scenic Railroad Commission, CO	ATL-09999-6-2392	09/22/06		$ 35,973	$ 35,973
New Bedford Economic Development Council, Inc., MA	ATL-09999-6-2589	09/22/06	$ 100,000		
Operation Hope, Inc., CA	ATL-09999-6-2653	09/22/06		483,494	
Puerto Rico Industrial Development Company	ATL-09999-6-2663	09/22/06		74,964	
Tri-County Economic Development District, WA	ATL-09999-6-2601	09/22/06	89,416		
The East Los Angeles Community Union and Subsidiary, CA	ATL-09999-6-2571	09/29/06	2,265,718		
National Institute of Standards and Technology					
PowerSicel, Inc., CO	ATL-09999-6-2115	04/05/06	42,386	30,382	20,453
Callida Genomics, Inc., CA	DEN-09999-6-1678	04/14/06		25,602	
Organ Recovery Systems, Inc., IL	ATL-09999-6-2111	06/26/06	22,496	9,619	
Siemens Westinghouse Power Corporation, FL	ATL-09999-6-1964	06/26/06		13,104	13,104
Gene Network Sciences, Inc., NY	ATL-09999-6-2461	07/24/06	59,688	20,502	
Display Technologies, Inc., CO	ATL-09999-6-2496	08/04/06		66,801	
InRAD, LLC, TN	ATL-09999-6-2526	08/11/06		82,362	
Integrated Fuel Cell Technologies, MA	ATL-09999-6-2406	08/21/06		142,301	
Engineous Software, Inc., NC	ATL-09999-6-2032	08/31/06		403,276	
Polymer Technologies, Inc., NJ	ATL-09999-6-2474	08/31/06	251,421	178,862	
Alfred University, NY	ATL-09999-6-2627	09/22/06		111,447	
COVA Technologies, Inc., CO	ATL-09999-6-2164	09/22/06	2,167	74,919	
Geometric Informatics, Inc., MA	ATL-09999-6-2357	09/22/06		13,944	

Appendix B 1. Processed Reports with Audit Findings (continued)

Report Title	Report Number	Date Issued	Value of Funds to Be Put to Better Use	Federal Amount Questioned	Federal Amount Unsupported
Intermet Corporation, MI	ATL-09999-6-2453	09/22/06		$ 211,016	
Intermet Corporation, MI	ATL-09999-6-2454	09/22/06		357,693	
MesoFuel, Inc., NM	ATL-09999-6-2372	09/22/06		119,479	
Molecular Nanosystems, Inc., CA	ATL-09999-6-2495	09/22/06	$ 13,160	13,573	
Motorola, Inc., AZ	ATL-09999-6-2227	09/22/06		12,765	
The Timken Company, OH	ATL-09999-6-2307	09/22/06			
E.I. du Pont de Nemours and Company, DE	ATL-09999-6-2523	09/29/06		977,033	
National Oceanic and Atmospheric Administration					
State of South Carolina	ATL-09999-6-2552	08/31/06	0	147,469	0
Federated States of Micronesia National Government, FM	ATL-09999-6-2672	09/22/06	0	37,215	37,215

REPORTING REQUIREMENTS

The Inspector General Act of 1978, as amended, 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	15–46
5(a)(2)	Significant Recommendations for Corrective Action	15–46
5(a)(3)	Prior Significant Recommendations Unimplemented	62
5(a)4	Matters Referred to Prosecutive Authorities	53
5(a)(5) and 6(b)(2)	Information or Assistance Refused	63
5(a)(6)	Listing of Audit Reports	56–61
5(a)(7)	Summary of Significant Reports	15–46
5(a)(8)	Audit Reports—Questioned Costs	54
5(a)(9)	Audit Reports—Funds to Be Put to Better Use	55
5(a)(10)	Prior Audit Reports Unresolved	63
5(a)(11)	Significant Revised Management Decisions	63
5(a)(12)	Significant Management Decisions with Which OIG Disagreed	63

Section 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. 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 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 management 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. There were five Census and three NIST reports more than 6 months old.

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.

TYPES OF OIG WORK PRODUCTS

The various kinds of audits, evaluations, inspections, and investigations at our disposal enable the IG's office to assess Commerce programs and operations from a range of perspectives. Thus we are able to provide program managers with reviews and recommendations that are either narrowly focused or comprehensive, as needed, 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. They may also involve reviewing the Department's financial assistance awards by assessing an award recipient's compliance with laws, regulations, and award terms; allowance of costs; and the degree to which projects achieved intended results.

Financial 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.

Attestation Engagements involve examining, reviewing, or performing agreed-upon procedures on a subject matter or an assertion about a subject matter and reporting the results. Attestation engagements can have a broad range of financial or nonfinancial focuses, such as an entity's compliance with laws and regulations; management's discussion and analysis presentations; and allowability and reasonableness of final grant and contract costs.

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.

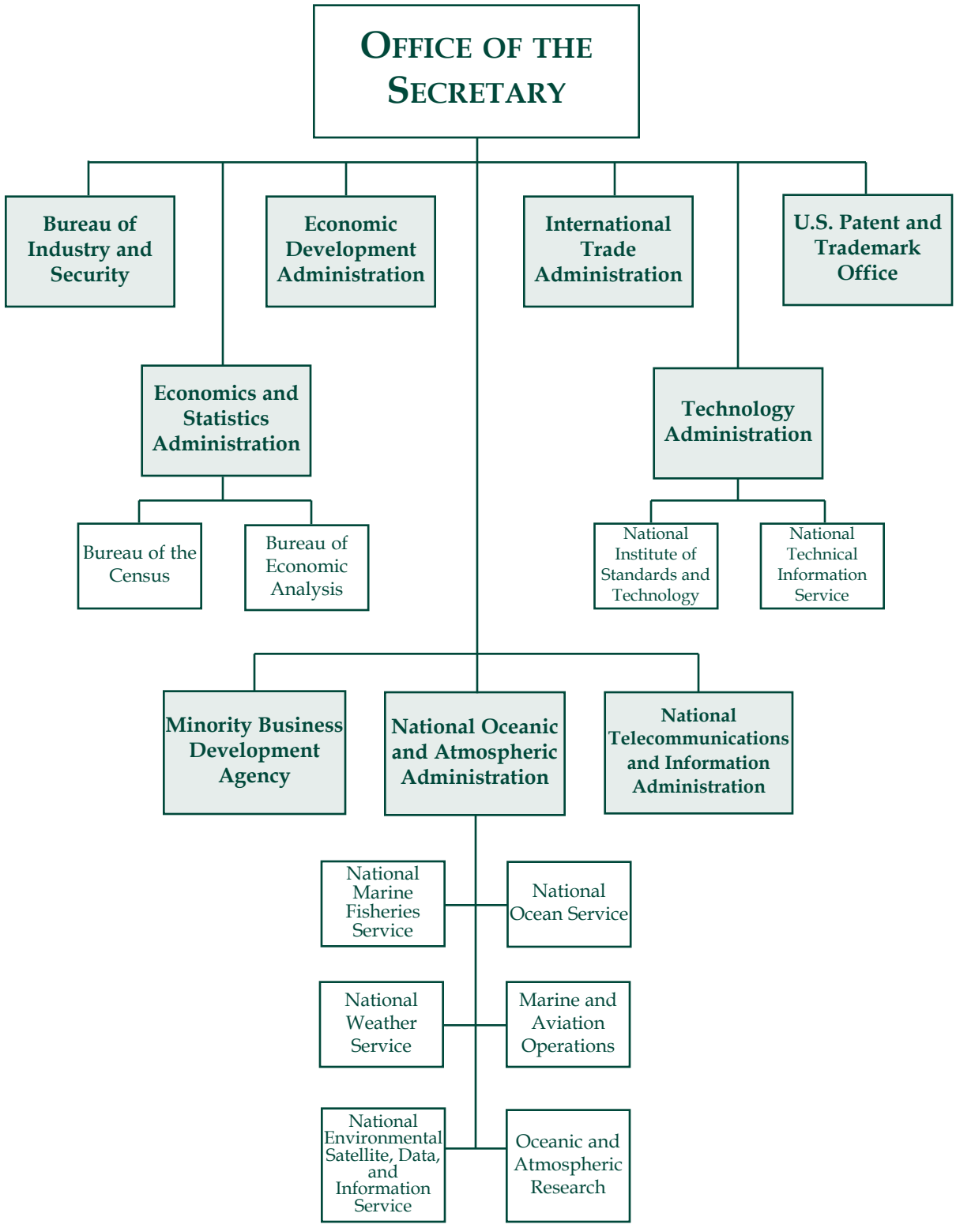
Systems Evaluations review system development, acquisitions, operations, and policy, focusing on computer systems and other technologies.

INVESTIGATIONS

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 violations 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.

U.S. Department of Commerce

The U.S. Department of Commerce creates the conditions for economic growth and opportunity by promoting innovation, entrepreneurship, competitiveness, and stewardship. The Department accomplishes its mission by providing national and local weather services, developing key economic and demographic data (including the decennial census), and working to advance technological and scientific innovation, protect and restore environmental resources, promote international trade, and support local, regional, and national economic development. These activities impact U.S. business and industry daily and play a critical role in the nation's economic well-being.



Commerce Headquarters
Washington, D.C.

OIG Regional Offices

Atlanta, GA

Denver, CO

Seattle, WA

U.S. Department of Commerce
Office of Inspector General
Room 7099 C, HCHB
1401 Constitution Avenue, N.W.
Washington, D.C. 20230
www.oig.doc.gov