

Semiannual Report to Congress

S E P T E M B E R 2 0 0 8



U.S. Department of Commerce
Office of Inspector General



IG's Semiannual Report to Congress

September 2008

CONTENTS

| | |
|--|----------|
| From the Inspector General..... | 1 |
| Major Challenges for the Department..... | 3 |
| Overcome the Setbacks Experienced in Reengineering Decennial Processes, and Conduct a Successful 2010 Census..... | 3 |
| Better Position the Department to Address Information Security Risks..... | 5 |
| Effectively Manage the Development and Acquisition of NOAA's Two Environmental Satellites..... | 6 |
| Establish a Safety Culture at NIST..... | 6 |
| Ensure NTIA Effectively Carries Out Its Responsibilities Under the Digital Television Transition and Public Safety Act..... | 7 |
| Other Issues Requiring Significant Management Attention..... | 8 |
| Work in Progress..... | 11 |
| Agency Overviews | |
| Economics and Statistics Administration..... | 13 |
| National Oceanic and Atmospheric Administration..... | 21 |
| United States Patent and Trademark Office..... | 31 |
| Department-Wide Management..... | 35 |
| Office of Inspector General | |
| Office of Investigations..... | 41 |
| Other OIG Activities..... | 43 |
| Tables and Statistics..... | 47 |
| Reporting Requirements..... | 54 |



Photo Courtesy Commerce Photographic Services

Commerce Herbert C. Hoover Building

FROM THE INSPECTOR GENERAL

We are pleased to present the Department of Commerce Office of Inspector General's *Semiannual Report to Congress* for the 6 months ending September 30, 2008. Much of our work during this reporting period focused on two priority areas for the Department: the 2010 decennial census and information security.

2010 Decennial Census

The Census Bureau experienced significant setbacks this past year, which led to the decision to abandon plans for using handheld computers for a major 2010 decennial field operation. Secretary Gutierrez asked the Office of Inspector General to (1) analyze the causes of problems with the Census Bureau's Field Data Collection Automation contract, (2) review plans and budgets to determine 2010 census high-risk areas, and (3) examine decennial decision documents and expenditures. We are nearing completion of reviews in all three areas and will promptly report our findings to the Secretary and Congress.

We recently issued two reports on high-risk decennial operations. The first was on the bureau's cost estimates for fingerprinting temporary census workers—a new undertaking for this decennial that is projected to cost \$148 million (see page 15). This estimate is hundreds of millions of dollars lower than earlier projections the bureau had developed, and reflects savings identified through our work and a concurrent analysis by Department and Census officials.

The second report, issued shortly after the close of the semiannual period, is on the bureau's dress rehearsal

test of its address canvassing operation. This operation is essential to, among other things, successfully delivering census questionnaires to U.S. households, and is estimated to cost \$500 million. The test revealed serious problems, and we recommended actions for mitigating them in the short time that remains before the actual 2010 operation begins. Our full report is available at www.oig.doc.gov and will be summarized in our next *Semiannual Report to Congress*.

We also issued a capping report highlighting the problems we've identified with 2010 operations in reviews conducted since the beginning of this decennial cycle (page 13). These early reports pointed to the potential for the kinds of problems the bureau is now confronting.

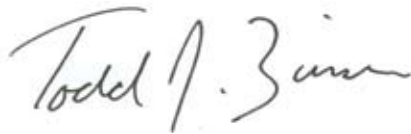
Information Security

We evaluated 10 information technology systems throughout the Department to meet the annual requirements of the Federal Information Security Management Act (FISMA). Information security has been a material weakness at Commerce since 2001. Last year, we worked with the Department to implement a 2-year plan for improving the certification and accreditation (C&A) process to eliminate the material weakness. The FISMA reviews we completed this year indicate that progress is being made: we concluded that, generally, Commerce's C&A process had improved. In order to eliminate the material weakness, the Department needs to ensure the progress continues until system C&As consistently meet required standards.

Other Areas of Focus

Among our other work during this reporting period, we completed a review of Commerce earmarks at the request of the Senate Subcommittee on Federal Financial Management, Government Information, and International Security. We assessed NOAA's National Data Buoy Center operations and NOAA's partnership arrangements with state agencies for enforcing fisheries regulations. And our ongoing international telemarketing fraud investigation resulted in another four convictions and more than \$94 million in fines and restitution. We also identified the top management challenges for the Department for fiscal year 2009. We briefly summarize those challenges here and will issue a full report.

We look forward to working with the Department to address these challenges. And we thank Secretary Gutierrez, senior officials throughout the Department, and members of Congress for their support of our work during this reporting period and for their responsiveness to our recommendations for improving Commerce operations.

A handwritten signature in dark ink, reading "Todd J. Zinn". The signature is written in a cursive, flowing style.

MAJOR CHALLENGES FOR THE DEPARTMENT

The Reports Consolidation Act of 2000 requires inspectors general to identify the top management challenges facing their departments. For FY 2009 Commerce OIG has identified five top challenges that require immediate and significant action from the Department, and four longer term issues that require its sustained attention. These challenges provide the focus for much of our work, as we assess the Department's progress in addressing them.

Challenge 1

Overcome the Setbacks Experienced in Reengineering Decennial Processes, and Conduct a Successful 2010 Census

The ability of the U.S. Census Bureau to successfully conduct its constitutionally mandated decennial count of U.S. residents in 2010 is at serious risk. After spending 8 years developing a completely new approach to census-taking—one that was to automate major field operations—the bureau scrapped plans for using handheld computer technology for the largest and most expensive of these operations, known as nonresponse follow-up, because of significant performance problems and loss of confidence in the Field Data Collection Automation (FDCA) contractor. It will now conduct this operation using paper and pencil, as it has done in previous censuses.

The inability of the bureau and its contractor to work together to produce a handheld computer and related systems for field data collection as originally envisioned, combined with major flaws in the bureau's cost-estimating methods and other issues, have added an estimated \$2.2 billion to \$3 billion to the original \$11.5 billion life-cycle cost estimate.

Top Management Challenges

- Overcome the Setbacks Experienced in Reengineering Decennial Processes, and Conduct a Successful 2010 Census
- Better Position the Department to Address Information Security Risks
- Effectively Manage the Development and Acquisition of NOAA's Two Environmental Satellites
- Establish a Safety Culture at NIST
- Ensure NTIA Effectively Carries Out Its Responsibilities Under the Digital Television Transition and Public Safety Act

The Department and the Census Bureau have taken significant actions during the past year to address problems, including extensive changes to decennial management, improvements in program management practices, and closer oversight of the decennial effort by the Department. However, despite these changes, significant risks remain for the 2010 decennial. Whether the bureau can in fact retool in time to conduct a reliable census, even at this increased price tag, represents in our view the most significant challenge facing the Department.

Census 2010 was to be the first high-tech count in the nation's history, with decennial employees using handheld computers to verify addresses through global-positioning software, collect data from house-

holds that did not mail back census questionnaires (i.e., nonresponse follow-up), and manage a variety of information and tasks. The handheld computers were the centerpiece of the strategy and other decennial operations were built around or impacted by the decision to use them. The switch to paper processes will require additional field staff and support personnel—which means more time to hire and train, and more dollars to do so. And it means Census must modify its other plans and operations to account for the change.

For example, address canvassing will remain automated, but will undergo its final operational test over an 8-day period, rather than the 3 months originally allotted. This operation is essential to, among other things, successfully delivering questionnaires and giving temporary staff accurate addresses and maps for nonresponse follow-up. Dress rehearsal testing of the



US Census Bureau

Address canvassers used the handheld computers to update maps and addresses in census testing, but the systems had significant problems. The time remaining for resolving the problems is extremely compressed.

operation—which concluded in June 2007—revealed serious problems, and plans for testing and enhancing the handhelds since dress rehearsal have been severely compressed. Address canvassing will undergo its final operational test over an 8-day period, rather than the 3 months originally allotted in the plan for the retooled census. We question whether Census will have the time to resolve issues arising from the 8-day test, scheduled for December, before the start of the 2010 operation. Training of address canvassers for the live operation commences in February 2009, leaving the bureau only a short period of time to fix any problems identified in this final test.

Help desk operations—key to ensuring the handhelds function properly during address canvassing—are just now in the process of being redesigned. Census is also taking over the regional census center communications infrastructure—which under the contractor has experienced numerous problems that must be resolved to ensure a successful 2010 count.

Overcoming automation-related issues is but one aspect of the challenge facing Census. The bureau must also address the readiness of numerous other operations that have suffered from inattention throughout the decade because of the greater than anticipated focus on automation problems. Census had to cancel tests of procedures for enumerating some traditionally difficult groups and settings, such as the homeless and military bases, while completed tests of others, such as American Indian reservations, have shown little effect on mitigating long-standing obstacles to producing accurate counts. Census cites the FY 2008 continuing resolution as the reason for cancellation of many of its planned tests.

In addition, the bureau must have a fingerprinting program in place prior to hiring the estimated 1.3 million temporary workers needed for field operations. Because the decision to fingerprint was made only recently, Census faces significant risks in implementing this \$148 million operation.

The overarching reason for the significant problems Census has encountered to date is the failure of Census Bureau management in place at the time to anticipate the complex IT requirements involved in automating the census. Contributing factors the De-

partment and Census must address include the insular nature of the bureau and lack of management with proven expertise in running complex programs and system acquisitions or applying contemporary private sector management methods.

With the first major decennial operation (address canvassing) beginning in early 2009, the new Secretary will have little time left for planning for the 2010 decennial, although he or she will have responsibility for its overall implementation. However, the new Secretary will have the opportunity to initiate planning for the 2020 census, using the lessons learned from the 2010 census.

Challenge 2

Better Position the Department to Address Information Security Risks

As in many federal agencies, putting proper information security controls in place has been an intractable problem at the Department of Commerce and a long-standing item on OIG's watch list. Despite additional expenditures to mitigate the problem, the Department has reported information security as a material weakness every year since FY 2001.

The reason for the material weakness is ineffective certification and accreditation (C&A): the Federal Information Security Management Act (FISMA) and OMB policy require agencies to certify that their systems and data are protected with adequate, functioning security controls before authorizing (accrediting) a system to operate. But year after year our FISMA reviews have found ineffective C&A processes that do not adequately identify and assess needed controls and ultimately fail to assure that systems and data are protected.

Securing systems from cyber threats is clearly the most difficult piece of the challenge, because these threats represent a moving target: they increase in number and sophistication almost daily. And as agencies incorporate wireless and other technologies to support their operations and workplace flexibilities, they invite new risks that must be anticipated and mitigated.

To be effective in this environment, the Department's IT security program must be proactive and fluid, staffed by IT security professionals who have the appropriate skills and experience to implement required security controls, assess their effectiveness, and anticipate and respond to emerging threats. They also need appropriate security clearances to effectively deal with potential cyber attacks. We have found IT security staff lacks adequate understanding of the Department's IT security policy, NIST standards and guidance, and security technology, and therefore cannot appropriately apply them. The Department cites lack of resources as a major impediment to improving IT security.

We have been working with the Department to eliminate the material weakness by the end of 2009 under a jointly developed plan that incorporates realistic milestones and measurable steps for building consistent and repeatable C&A practices. A key element of the strategy is continuous monitoring, which requires agencies to regularly assess and adjust their security controls to maintain or improve protective measures. Our FISMA reviews this year noted improvements, but still fewer than half the systems we evaluated met FISMA standards. However, several showed subsequent improvements because of rigorous continuous monitoring activities.

The Department has made progress toward implementing the Cyber Security Assessment and Management tool—a software application developed by the Department of Justice that allows users to take a 360-degree approach to C&A. They can input system information as they begin the C&A process, and, among other things, generate and implement a security plan that complies with FISMA requirements, analyze security requirements, and track resolution of vulnerabilities and the results of security control monitoring. The systems we reviewed this year were certified and accredited without the benefit of the tool. But once fully integrated, the tool should bring greater consistency to the C&A process across all Commerce bureaus.

Challenge 3

Effectively Manage the Development and Acquisition of NOAA's Two Environmental Satellites

NOAA is modernizing its environmental monitoring capabilities, spending billions of dollars on two satellite systems that provide critical data: the National Polar-orbiting Operational Environmental Satellite System (NPOESS) and Geostationary Operational Environmental Satellite-R Series (GOES-R).

Space acquisitions like NPOESS and GOES-R are highly technical and complex and have a history of cost overruns, schedule delays, and performance failures. The costs and schedules of both of these systems have significantly increased since the projects commenced. They therefore require careful oversight to minimize any further disruption and to prevent any gaps in satellite coverage—a situation that could have serious consequences for the safety and security of the nation.



The \$12.5 billion NPOESS project will provide continuous weather and environmental data for longer term weather forecasting and climate monitoring through the coming 2 decades.¹ The initial plan called

for the purchase of six satellites at a cost of \$6.5 billion, with a first launch in 2008. But problems with a key sensor—the Visible/Infrared Imager Radiometer Suite (VIIRS)—were a major contributor to the current \$12.5 billion estimate, while the number of satellites was reduced to four and the first launch pushed back to 2013. Recent analysis indicates that the \$12.5 billion estimate could substantially increase in the near future.

The \$7.7 billion GOES-R system will offer an uninterrupted flow of high-quality data for short-range weather forecasting and warning, and climate



¹The cost of the NPOESS program is shared equally by NOAA and the Department of Defense.

research through 2028. An inadequate acquisition and management process contributed to underestimated costs for GOES-R and planned satellite capabilities that were too ambitious. As a result, the projected cost of GOES-R has increased from \$6.2 billion to \$7.7 billion, a major sensor has been removed, and the number of satellites to be purchased has decreased from four to two.

Reining in additional costs and delays in both programs requires very specific action and vigilant oversight. For NPOESS, the three agencies developing the system—NOAA, NASA, and the Department of Defense—must (1) control and resolve the continuing problems with VIIRS, and (2) improve triagency decision making. Because NPOESS is the only source of critical weather and environmental data, it is especially important that VIIRS problems be resolved and congressional confidence in and support of the program be maintained.

For GOES-R, NOAA needs to (1) work closely with the Department to ensure they follow best practices in overseeing the acquisition while awaiting development of formal Commerce oversight policies and procedures to guide such projects, and (2) work with Congress to update the baseline life-cycle cost estimate used in its annual reporting on the satellite system.

Challenge 4

Establish a Safety Culture at NIST

A June 2008 plutonium spill at the National Institute of Standards and Technology's Boulder, Colorado, laboratory raised serious concerns about NIST's ability to perform state-of-the-art research with radioactive and other dangerous materials while protecting the safety of workers and the community at large.

The plutonium spill was one of several incidents reported at NIST labs in the past few years that have revealed management flaws and a lax safety culture at the agency. But it was by far the most serious in terms of the potential for widespread harm.

The plutonium spill prompted a series of reviews by independent health and safety experts, the Depart-

ment of Energy, and NIST's Ionizing Radiation Safety Committee, all of which shared a common finding—a commitment to safety at NIST Boulder is seriously lacking.

Two studies conducted by NIST have identified a backlog of more than \$500 million in facility maintenance and repair requirements. A 2004 study found \$458 million in deficiencies at NIST's Gaithersburg campus and a 2008 study identified \$48 million in deficiencies at Boulder. Many of the items relate directly to safety. NIST noted that it should be investing at least \$50 million to \$70 million annually to bring its facilities to a “fair” condition and stay ahead of further deterioration. According to the Department, NIST received \$32 million for facilities in FY 2008.



NIST

According to a 2008 study, the NIST Boulder campus, pictured above, had \$48 million in facility deficiencies, many of them related to safety.

It is clear from the circumstances surrounding the plutonium incident and subsequent revelations that, at a minimum, NIST must make safety a primary concern at all organizational levels and strictly comply with all federal requirements and industry standards. It must establish and enforce stringent policies and procedures for handling hazardous materials and strict lines of accountability for implementing them.

Challenge 5

Ensure NTIA Effectively Carries Out Its Responsibilities Under the Digital Television Transition and Public Safety Act

The Digital Television Transition and Public Safety Act of 2005 assigned the National Telecommunications and Information Administration responsibility for implementing a \$2.5 billion initiative for the conversion to digital television and improvements to public safety communications. The act authorizes NTIA to use \$1.5 billion to support the nation's February 2009 switch to all-digital broadcasting by offering coupons toward the purchase price of converter boxes that will enable analog television sets to receive digital broadcasts.

A primary purpose of the switch is to free up radio frequencies for advanced wireless emergency communications at state and local levels. NTIA will use approximately \$1 billion to fund grants for public safety interoperable communications (PSIC) projects in all 50 states, the District of Columbia, and the U.S. territories—a total of 56 entities.

The authorizing legislation requires NTIA to coordinate with the Department of Homeland Security in administering the PSIC program and set a statutory deadline of September 30, 2010, to expend grant funds. Subsequent legislation set a statutory deadline of September 30, 2007, for the award of grants.

Converter Box Coupon Program Is Progressing

NTIA has made substantial progress in preparing television viewers for the switch to digital broadcasting by dispensing up to two \$40 coupons per household to offset the purchase price of the converter boxes, which enable analog TVs to receive digital signals. NTIA contracted with IBM to provide certain services to implement the coupon program, and had issued more than 26 million coupons as of September 30, 2008, and redeemed 10 million of them.

Maintaining strict accountability for funds in a program of this type and size requires careful oversight and strong internal controls to, among other things, guard against waste, fraud, and abuse among retailers, and to adapt to evolving program requirements.



OIG

This communications tower was erected by an Arkansas PSIC grantee as part of its interoperable communications project. Obtaining FCC licenses to build these towers and meeting various state and local requirements can add months or years to a project's time frame.

Although administering the coupon program is NTIA's primary role, the act authorizes the agency to use up to \$5 million for outreach and education to ensure that consumers know about both the digital TV transition and the coupons. Although the Federal Communications Commission has primary responsibility for consumer education and outreach, NTIA should continue to work with stakeholders, including representatives of groups at risk of finding themselves without television reception on February 17, 2009, to ensure a smooth transition to digital television.

PSIC Grantees May Not Be Able to Finish Projects Within the Mandated Time Frame

The PSIC program is a one-time grant opportunity to target specific funds and resources toward improving the interoperability of local and state voice and data communications. But grantees are moving slowly, and whether they can complete their projects by the statutory deadline of September 30, 2010, is questionable.

As of September 2008, grantees had spent less than 1.5 percent of the available \$1 billion, which leaves them only 2 years to complete their projects or lose funding. In September and October 2008 we contacted 22 grantees, including 19 of the 20 receiving the

largest grants. Only one stated that it plans to acquire most of its interoperable communications equipment within the next 6 months. Eight told us they are in the early stages of planning their acquisitions. The other 13 will start acquiring most of their interoperable communications equipment in late FY 2009 or possibly at the beginning of FY 2010. Given all that must follow the purchase of equipment—installation, operational testing, and training at a minimum—grantees who are still in the acquisition stage as late as FY 2010 face the very real possibility of arriving at the program's September 30 deadline with partially completed projects but without funding to finish them out.

NTIA should expeditiously identify grantees who are at high risk of not meeting the statutory deadline for completing their projects, give them the technical assistance they need to accelerate the process, carefully monitor their progress, and keep Congress informed of the PSIC program's status toward achieving its objectives. If any entities seem still unlikely to meet the deadline, NTIA should work with Congress to extend it.

Other Issues Requiring Significant Management Attention

Several other Commerce operations and activities present longer standing challenges, and their resolution is essential to the Department's sound management and mission success. The first—acquisition management—has ramifications Department-wide. The remaining three—though agency-specific—have a direct bearing on Commerce's missions relating to U.S. economic strength and competitiveness, or national security.

Weaknesses in the Department's Acquisition Oversight and Acquisition Workforce

Acquisition and contract management has been a persistent watch list item for inspectors general and GAO, as related government spending has ballooned in recent years. Spending on contracts government-wide, for example, has more than doubled since 2000—from \$208 billion to \$430 billion in FY 2007. Meanwhile, the federal acquisition workforce has remained fairly constant, and the projects it supports

have greatly increased in complexity and risk.

Over the next 2 years, the Department of Commerce will spend an average of approximately \$3 billion annually on goods and services. The 2010 decennial census and two critical NOAA satellite systems will account for roughly a third of these annual expenditures. All three of these programs have already suffered significant cost overruns and schedule delays because of weaknesses in acquisition management.

The Department does not have coherent policies to guide systems acquisition or effective oversight mechanisms, and these failings were major contributors to the problems we identified with NOAA's GOES-R satellite program and the Census Bureau's field data collection automation contract. Commerce also lacks a sufficient amount of skilled contracting and project management expertise.

The Department is working to address these problems, but the process is slow and in its early stages. Commerce is strengthening acquisition and contracting by updating its antiquated policies and procedures to promote more effective planning, implementation, and oversight. It is also taking steps to make better use of its oversight bodies—the Acquisition Review Board and the Commerce Information Technology Review Board—and to ensure acquisition plans are appropriate, and programs and contracts are reviewed at key decision points in their life cycle.

But success in these efforts will not be enough to improve the Department's overall acquisition operations without commensurate success in hiring and retaining a qualified acquisition workforce. The Department needs a comprehensive human capital strategy that (1) taps into government-wide recruiting initiatives, (2) explicitly defines what acquisition skills and competencies it needs and how they will evolve over the short and long term, and (3) offers professional development and other incentives to attract and keep qualified candidates.

USPTO's Long and Growing Patent Processing Times, and Its Financing Vulnerabilities

The efficiency with which the U.S. Patent and Trademark Office processes patent applications has a direct bearing on how well it achieves its mission of promoting U.S. competitiveness. Meeting the demand for new patents in a timely manner has been a long-standing challenge for USPTO. Increases in both the volume and complexity of patent applications have lengthened application processing times and backlogs dramatically. In 2004, USPTO had a patent backlog of nearly a half-million applications and processing times of 27 months. By 2007, processing times averaged nearly 32 months, with wait times for communications-related patents as long as 43 months.

As of September 30, 2008, USPTO reported a backlog of 750,596 applications and estimated that the backlog will exceed 860,000 by September 2011. USPTO needs to reverse the upward trend and continue to implement measures discussed in its 2007-2012 strategic plan that have a significant impact on reducing the backlog, such as shortening application review times, improving examiner error rates, and hiring, training, and retaining skilled examiners.

USPTO's unique financing structure also presents challenges. There is a complex relationship between the number of patent applications filed, the size of the application backlog, the number of patents issued, and the fees USPTO collects in connection with the patent process. The agency uses fees collected today to pay for patent applications filed and examined in prior years. With the backlog growing, processing times increasing, and the number of patents issued flattening, this method of financing could become increasingly risky because of the potential shortfall in future fee collections. The current model for financing USPTO's critical mission warrants attention to ensure that it will continue to provide sufficient funding to process all backlogged applications as well as any newly filed.

NOAA's Ability to Conserve the Nation's Fragile Oceans and Living Marine Resources While Ensuring a Vital U.S. Commercial Fishing Industry

According to NOAA, 3.5 million square miles of our coastal and deep ocean waters and the Great Lakes support over 28 million jobs—one of every six—in the United States, and the value of the U.S. ocean economy tops \$115 billion. But these economic benefits come at great cost as the health of our ocean and coastal ecosystems continues to decline in the face of increasing coastal development, pollution, overfishing, and the destructive impact of invasive species.

Charged with maintaining and improving the viability of marine and coastal ecosystems while supporting global marine commerce and transportation, NOAA manages a significant portion of the federal government's investment in living marine resources. It faces difficult challenges in promoting the health of these resources while ensuring they sustain the vital economic benefits we derive from them.

In January 2007, the President signed the reauthorized Magnuson-Stevens Fishery Conservation and

Management Act, which requires annual catch limits, an end to overfishing by 2011, and better integration of fishery management planning with national environmental review procedures to ensure the environmental impacts of any significant ocean activity under consideration are thoroughly vetted. The success of these new requirements in improving the status of our marine resources depends on how effectively NOAA can enforce them without undermining the health of the U.S. fishing industry. To fulfill its mandates for living marine resources, NOAA also needs to take action to rebuild populations of protected species, conserve important habitats, and undertake the science programs necessary to improve its understanding of complex marine ecosystems.

BIS' Setbacks in Modernizing Its Obsolete Information Technology Infrastructure to Strengthen the Dual-Use Export Control System

In January 2007, GAO added the Bureau of Industry and Security's dual-use export control system to its government-wide high-risk list. One of the key challenges facing BIS in ensuring that the dual-use export control system is properly equipped to advance U.S. national security, foreign policy, and economic interests is the replacement of its obsolete Export Control Automated Support System (ECASS). BIS' core export administration and enforcement business processes are directly supported by ECASS. Approximately 450 federal staff and 28,000 exporters currently use the system. However, the database structure—originally deployed in 1984—is complex and no longer supported by the technology industry. The effort to modernize ECASS began in 1996, but the project has been beset by technical problems, schedule slips, and funding shortages that current management has been attempting to address in a budget-constrained environment.

The current projected completion date for the ECASS modernization is FY 2014. Based on our interviews, the total funding requirements for ECASS modernization are not clearly established. BIS must provide a comprehensive plan for what is required to modernize ECASS, including how much it will cost and how it will avoid the management and technical problems



experienced in past modernization attempts.

Enhancing the performance of ECASS and ensuring continued operation of an effective licensing information system are far too important to postpone any longer. BIS must demonstrate that it has a modernization strategy and plan in place to convincingly make the case for increased funding, or develop a plan to implement its ECASS modernization effort with existing resources (i.e., reallocate existing funding).

Work in Progress

During this reporting period, the Office of Inspector General initiated the following audits and evaluations:

BIS

IT Infrastructure System

Determine whether continuous monitoring of information security controls is (1) keeping the authorizing official sufficiently informed about the operational status and effectiveness of security controls; and (2) resulting in prompt mitigation of any identified security control deficiencies. Also assess whether BIS has resolved deficiencies we identified in our FY 2006 Federal Information Security Management Act evaluation.

Issues Related to the Bureau of Industry and Security's Budget and Responsibilities for International Treaty Implementation and Compliance

Review budget management practices in the Bureau of Industry and Security related to international treaty implementation and compliance activities.

Census

2010 Decennial Census Reviews in Response to Commerce Secretary's Request

- *Field Data Collection Automation Contract.* Determine (1) why cost estimates have increased while the scope of the contract has been reduced; (2) why funds were not available for the contract to proceed as planned; and (3) what went wrong with processes for

defining requirements and developing and testing systems.

- *High-Risk Decennial Activities.* Review cost, schedule, and performance/quality issues, with the goal of providing timely analysis and recommendations for decision makers.
- *Decision Documents and Expenditures.* Identify the decision documentation and other information used to support allocations and spending for the 2010 census and determine whether they are consistent with planned activities and budget requests.

2008 Dress Rehearsal Test of Address Canvassing Operation

Determine the extent to which address canvassing improved the accuracy of the master address file—the comprehensive, nationwide listing of addresses the bureau will use to contact households either via mail or in person to collect census data.



NIST

Policies and Procedures for Handling Radioactive Materials

Evaluate NIST's training, safety, and response policies and procedures relative to radioactive materials as well as controls over its inventory of and access to these materials. Also assess whether the agency's management structure facilitates incident preparedness and response, and the extent to which security and emergency protocols protect the health and safety of NIST employees at research labs and the surrounding communities.

NOAA

National Marine Fisheries Service's Northeast Fisheries Science Center

Evaluate NMFS' implementation of National Standard 2 of the Magnuson-Stevens Fishery Conservation and Management Act, which requires that conservation

and management measures in fishery management plans be based on the best scientific information available. In particular, we are assessing the extent to which the “best available science” has been used in developing fishery management plans and NMFS’ procedures for responding to data requests from the public.

Fisheries Finance Loan Program

Audit the operation and effectiveness of the direct loan portion of this NOAA program, which accounts for \$412 million of the total amount of loans approved since the program’s inception in FY 1997.

Facility Replacement Alternatives for NOAA’s Southwest Fisheries Science Center

Evaluate NOAA’s cost-benefit analysis for selecting from among the three options it is considering for replacing one of the center’s buildings.

Policies for Disseminating Research Data

Assess Department and NOAA policies regarding public release of research data in general, as well as the events surrounding a NOAA web site article and follow-up fact sheet on Atlantic hurricanes and climate.

NTIA

Management of Public Safety Interoperable Communications (PSIC) Grant Program

Assess management of the Public Safety Interoperable Communications grant program by NTIA and the Federal Emergency Management Agency and report to Congress as required by amendments to Section 3006 of the Digital Television Transition and Public Safety Act of 2005 (Title III of the Deficit Reduction Act of 2005, Pub. L. No. 109-171).

Audits of Arkansas, Louisiana, Nevada, and Pennsylvania Public Safety Interoperable Communications Grants

Determine the progress these states have made in acquiring and deploying interoperable communications with PSIC grant funds and whether their use of these funds is meeting all federal requirements.

Converter Box Coupon Program

Assess the adequacy of NTIA’s controls to prevent waste, fraud, and abuse in the program, and the effectiveness of its program and contract oversight.

USPTO

Quality Assurance Process

Determine (1) the effectiveness of USPTO’s patent quality assurance process in ensuring that established standards of patent examination quality are met, and (2) whether the process complies with applicable Department, bureau, and federal laws, regulations, policies, procedures, and guidelines.

FY 2008 Financial Statements and Information Technology Controls

Determine whether the financial statements are fairly stated in accordance with generally accepted accounting principles. These audits are performed by an independent public accounting firm, under OIG oversight.

Department-wide

FY 2008 Consolidated Financial Statements, Information Technology Controls, and Special Purpose Statements

Determine whether the financial statements are fairly stated in accordance with generally accepted accounting principles. These audits are performed by an independent public accounting firm, under OIG oversight.

Grants Oversight

Assess oversight activities designed to detect and prevent fraud in the various grant programs administered by EDA, NIST (NIST and NTIA grants), and NOAA (NOAA, ITA, MBDA, and Office of the Secretary grants); and consider the Office of Acquisition Management’s role in the grants process, which includes developing, coordinating, and overseeing Commerce’s financial assistance policy, and implementing government-wide grants policy directives at the Department.





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:

The *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.

The *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.

2010 Decennial Census: OIG Reviews Through the Decade Identify Significant Problems in Key Operations

The Census Bureau's announcement last April that it would not use handheld computers to count Americans who do not return 2010 census questionnaires and the \$2.2 billion to \$3 billion increase in the estimated life-cycle cost made it clear that the 2010 census was at risk. The Office of Inspector General issued a briefing report on the work we had conducted on the decennial census to that point: the six reports we issued between 2000 and April 2008 highlighted a series of continuing problems in the areas of contracting, maps and address lists, systems development, and

enumerating hard-to-count populations. We summarized our major findings as follows. Census's response to our findings and recommendations are presented in the individual reports, which are available at www.oig.doc.gov.

Field Data Collection Automation (FDCA) Contract (OSE-17368, OIG-17524)

The Census Bureau's decision in 2001 to automate certain major operations for the 2010 decennial posed significant risks while offering considerable potential efficiencies, savings, and improvements in the count. The handheld computers Census proposed using were the centerpiece of its reengineered field operations. But problems with their development have led to an enormous growth in the estimate to complete the FDCA contract and have impacted the entire 2010

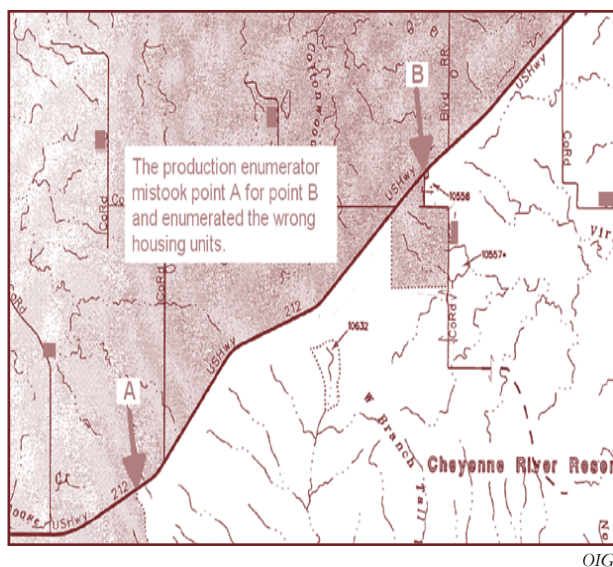
operational plan. In 2005, we reported numerous issues with the acquisition process for the handheld devices. Census had originally intended to develop them in-house and tested prototypes in both 2004 and 2006. The devices and related systems had serious problems in both tests, including crashes, slow response times, and lost data. These experiences should have better informed the bureau's efforts to define requirements for the contractor. Since letting the contract, Census has changed and added numerous requirements before finally abandoning plans to use these devices for nonresponse follow-up.

Maps and Addresses (OIG-17524, OSE-18027, OSE-15725)

Developing an accurate master address file (MAF) and maps has been a long-standing problem for the bureau. Our reviews have found numerous instances in which enumerators are sent into the field with incorrect maps and address information.

Map and Address Reliability

In Census 2000, the master address list contained millions of duplicates. Our 2008 review of the address canvassing operation conducted during dress rehears-



Four people attempted to sort out this area using maps that lacked landmarks and some roads. They introduced numerous errors to the housing information.

al continued to find errors in the lists that resulted in duplicate addresses or missed housing units.

Inadequate maps and address lists were an issue during the 2006 test of update/enumerate—the paper-based operation Census uses to survey American Indians living on reservations—and these tools were a key factor in the operation's failure to improve the population count. We found that enumerators often could not locate households because maps lacked current community landmarks and other details that help one navigate large rural communities devoid of traditional postal addresses. The bureau had expected the handheld devices to facilitate its ability to improve map details and address lists during address canvassing. But the technical problems with the systems we noted in both the 2004 and 2006 tests prevented field staff from making the extensive corrections needed. To compensate for the map deficiencies, we recommended that the bureau equip enumerators with handheld computers containing GPS for navigation and the GPS coordinates collected during address canvassing.

System and Software Development

Shortly after the 2000 census, the Census Bureau initiated an in-house upgrade of the technology supporting MAF/TIGER¹ to improve map and address accuracy for 2010. We evaluated the upgrade project in its early stages, and found that the bureau did not have an effective management process in place at the project's inception: system requirements, a work plan, and project schedule were not developed in tandem, and this complex redesign got a late start. We also found that the bureau's software development process did not follow key industry standards and best practices for minimizing risk.

Quality Control

Without sound quality control procedures, Census lacks assurance that field operations are working as intended and the data collected is reliable. Our reviews of census operations tested in 2006 recommended some enhancements to the quality check for group quarters address lists to improve their accuracy, and to quality procedures in update/enumerate to better identify missed housing units. In the 2008 dress rehearsal, the bureau greatly streamlined quality control procedures

¹ TIGER stands for Topologically Integrated Geographic Encoding and Referencing.

for address canvassing, but technology problems prevented Census from collecting reliable data to assess and improve the procedures before 2010.

Hard-to-Count Populations (OSE-18027, IPE-18046, OIG-16949)

The Census Bureau develops separate operations that target people who are especially difficult to count, such as the homeless, or those who live in remote areas or in certain types of group situations (e.g., prisons, college dormitories). We evaluated the 2004 and 2006 tests of several of the operations.

Update/Enumerate

This operation is used to survey reservations and other sparsely populated, remote locations, and update maps and addresses. Our review of the update/enumerate operation tested in 2006 evaluated the impact of a change to better capture reservation household size and found it to be ineffective, ultimately adding only one person to the total number of residents in these households.



Small residential group quarters often blend into single family neighborhoods and are incorrectly enumerated. This convent in the Austin, TX, test site was not counted as a group quarters.

Group Quarters

People who live in group situations (college dormitories, nursing homes, prisons, and group homes) are hard to count accurately, partly because developing precise criteria for identifying who to include in this group is difficult. Our review of the group quarters enumeration approach tested in 2004 found the bu-

reau made little progress in improving its ability to count this population: criteria were ambiguous and were developed after training materials had been prepared. The materials therefore did not offer adequate instruction on how to differentiate and properly categorize certain types of group homes.

Census addressed some of these problems in the 2006 test. It developed and verified a list of group quarters and either helped residents complete the form, left census questionnaires to be picked up at a later time, or used administrative records to fill in the needed information. Even so, the response rate among certain groups was low. (OIG-19217)

Plans, Costs for Fingerprinting Temporary Staff Remain Uncertain

Census must conduct background checks to assess the suitability of all temporary decennial employees. For the 2010 decennial, Census plans for the first time to submit applicants' fingerprints along with background check requests to meet the requirements of the National Crime Prevention and Privacy Compact Act of 1998. The Compact generally requires that biometric information accompany requests for criminal history records that are being accessed for purposes unrelated to criminal justice matters, such as determining employment suitability. The bureau expects to hire 1.3 million temporary workers to conduct the 2010 census. The FBI estimates that about 1 percent of these workers—or 13,000—will have criminal backgrounds that will not be correctly detected by a name check alone.

Fingerprinting will help mitigate the risk of hiring temporary employees with unsuitable backgrounds, but it is a major new operation for the decennial census that could cost hundreds of millions of dollars. Census has developed several cost estimates for the operation that reflect different assumptions and operational plans. We examined its April 1, 2008, estimate of \$494 million to identify possible cost reductions and recommended a number of cost-cutting measures, which we summarize here and which the

bureau incorporated in a subsequent estimate released on May 1.

A more pressing concern, however, is that operational plans and funding for satisfying legal requirements under the Compact remain unresolved. We first urged Census and the Department to resolve the fingerprinting issue promptly in February 2008 and reiterated our concern in our March 2008 Semiannual Report to Congress. Commerce's June 2008 amended FY 2009 budget submission to Congress included \$10 million for "exploring options to most efficiently incorporate fingerprinting into [the bureau's] overall screening process." According to the May cost estimate, Census will need \$56 million for fingerprinting during FY 2009. The continuing uncertainty surrounding fingerprinting plans increases operational risks and makes it impossible to accurately estimate and budget for decennial operations.

Census shaves nearly \$100 million from estimate in response to OIG analysis

Our review of the April 1 estimate found that the number was inflated by \$46.1 million because Census had double-counted certain administrative costs. We also identified measures for reducing costs of examiner training and fingerprinting kits, for another \$53.5 million in savings. Specifically, we suggested that the bureau hold several "administrative" days, during which examiners fingerprint temporary hires, rather than just one such day as originally intended. This would reduce the number of examiners and fingerprinting kits needed, and thus reduce associated training and materials costs. The examiners would fingerprint several groups of temporary staff over successive days and reuse their fingerprinting kits at each session.

Census's May estimate eliminated the double-counted cost and assumed two administrative days, which cut the number of examiners by about 60,000 and saved \$30.5 million in related training costs. It changed its cost model assumptions to account for reusing fingerprint kits, for a savings of \$23 million.

Department and Census decide to make other changes

Concurrent with our review, the Department also worked with Census to identify possible savings. Like OIG, the Department suggested that Census reuse some fingerprinting kits, specifically, those purchased to fingerprint recruits hired for operations that precede nonresponse follow-up (e.g., address canvassing). In addition, Department and Census officials decided on the following changes:

- Reduce the assumed travel time and distance for temporary employees' commuting to administrative sessions, which reduced the May estimate for mileage reimbursement. However, we note that neither the April nor May estimates for travel time and distance are supported by benchmark data from Census 2000.
- Cut class sizes from 16 to 12, which shortened the time examiners need to fingerprint the class.
- Reduce the number of scanners needed for scanning fingerprint cards and the fees paid to the FBI for conducting the checks.
- Modify assumptions for handling personally identifiable information, shipping the fingerprint cards, and hiring a contractor to train examiners.

These adjustments accounted for another \$46.4 million reduction in the May estimate.

Additional savings may be possible

While the May projection was substantially lower than the April one, we found that the estimate for processing fingerprinting kits should have been \$3.5 million lower to reflect the purchase of fewer kits. We also noted that costs for examiner training and scanning equipment could be cut further if the bureau adds additional administrative days.

Our Recommendations

We recommended that the Department and the Census Bureau do the following:

1. Finalize plans and cost estimates for fingerprinting temporary workers during 2010 that comply with all applicable legal requirements in order to reduce uncertainty and the associated operational and budget risks.
2. Assess the cost and operational implications of processing fewer fingerprint kits, adding more administrative sessions, and reducing the number of scanners required as more sessions are added.
3. Further evaluate the time and distance assumptions required for travel to training locations to ensure that they are consistent with available benchmark data from the 2000 decennial.

Bureau Response

Census officials stated that they, along with the Department, have considered our recommendations and made progress toward specifying the operational procedures and estimated costs of fingerprinting for the 2010 Census. (*OIG-19058-1*)

FISMA Reviews at BEA and Census Identified Certification and Accreditation Weaknesses, But Continuous Monitoring Leads to Improvements

To meet FY 2008 FISMA reporting requirements, we evaluated the certification and accreditation of the Bureau of Economic Analysis's Estimation Information Technology System (BEA-EITS), Census's Wireless Data Communications General Support System, and the Field Data Collection Automation system. We also tested selected security controls on BEA-EITS and the Wireless Data Communications system.

To gauge the impact of continuous monitoring—a process that is emphasized in the latest FISMA guidance—we revisited the BEA system after our C&A

work concluded to determine whether continuous monitoring was in fact having the desired effect of mitigating the deficiencies we had identified. We found that it was: many of the problems noted in our C&A review had been corrected.

The results of our FISMA work at BEA and Census are summarized below.

Testing Security Controls and Tracking Vulnerabilities Among Weak Points in BEA Certification Process

BEA-EITS handles all of the bureau's mission-related information technology operations and data—much of which is of critical importance to the nation. According to its own description, BEA “produces some of the most closely watched U.S. economic statistics that influence critical financial decisions made by governments, businesses, and households.” BEA-EITS supports the agency's core business processes of collecting, analyzing, tabulating, and disseminating data.

Our review found that the system security plan was adequate to support the certification process. But the resulting certification had a number of weaknesses:

- It lacked credible supporting evidence that security controls on system components were properly tested to verify they were implemented correctly and operating as intended.
- It did not include some significant system vulnerabilities in either the security assessment report or in the agency's plan of action and milestones (POA&Ms) document.

Our own assessment of a set of system components found significant security control weaknesses that BEA's certification did not identify.

We concluded that BEA needs to, among other things, improve security control assessments to (1) include adequate detailed and credible validation of the assessments' scope, procedures, and outcomes for specific system components; (2) comply with Department

policy and FISMA guidance for tracking and correcting system security weaknesses; and (3) clearly articulate in the C&A documentation the vulnerabilities for which the bureau is accepting risk.

Bureau Response

BEA did not specifically indicate whether it agreed with our findings (with the exception of the need to better track security weaknesses), and its proposed corrective actions are not fully responsive to our recommendations. The bureau did indicate its intention to use our recommendations to improve BEA information security, and noted that it has improved its continuous monitoring program to ensure it assesses the effectiveness of security controls on all system components. (*OSE-19001*)

Why Is Continuous Monitoring Important?

A critical aspect of the security authorization process is the post-authorization period involving the continuous monitoring of an information system's security controls (including common controls).

The ultimate objective of the continuous monitoring program is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. Continuous monitoring is a proven technique to address the security impacts on information systems resulting from changes to the hardware, software, firmware, or operational environment.

*NIST Special Publication 800-37
Guide for Security Authorization of Federal Information Systems
A Security Life Cycle Approach
August 2008*

Improved Security Control Assessments Needed for Otherwise Acceptable Census C&A Process

The Wireless Data Communications system enables office automation, communications, file access, and other services for approved wireless devices. The system comprises two wireless network domains: a secure network that handles day-to-day business information and is restricted to sworn Census employees and a guest network that permits non-Census personnel to access the Internet.

Our review showed the system security plan was generally adequate and certification assessments were generally effective and comprehensive but some improvements were needed in both: several control descriptions in the security plan did not fully address control requirements, some controls were inaccurately identified, and some assessment procedures were not sufficient to validate all control requirements.

In addition, our own assessment of system components uncovered vulnerabilities in five areas that required remediation. We concluded that the certification was sufficient for the authorizing official to make a credible, risk-based decision to approve system operation, but Census needs to improve security control assessments.

Bureau Response

Census concurred with our recommendations but took exception to four of the vulnerabilities we identified during our tests of system components. The bureau contended that one of the four is not applicable to the system, but we disagreed and reiterated our recommendation that it be remediated. Census stated that the remaining three—which pertain to system access, user identification and authentication, and audit logs of system activity—cannot be remediated because the system cannot support the necessary changes. However, the bureau subsequently agreed that one of the three could be resolved and indicated it is taking steps to do so. We again reiterated the need for addressing the other two in order to optimize the system's security status. (*OSE-19163*)

Inadequate C&A for Field Data Collection Automation System

We evaluated the certification and accreditation of the FDCA system as configured to support address canvassing during FY 2008 dress rehearsal operations. This C&A is the first of at least three that Census will complete before the system's final configuration for the 2010 decennial.

We found the system security plan was generally adequate but the bureau began certification assessments several months before the plan had been approved. We also found the bureau had not defined secure configuration settings for a number of system components, had not evaluated established settings for others, and did not test several security controls. Finally, vulnerabilities discovered during the C&A process were not included in either the security assessment report or the plan of action and milestones, which means the authorizing official approved the system's operation without complete, accurate information regarding its security status.

We recommended that Census ensure certification and accreditation do not commence until the security plan has been approved, secure configuration settings for all system components are defined and evaluated, all security controls tested according to applicable procedures, and identified vulnerabilities reported and tracked on the system POA&M.

Bureau Response

The Census Bureau concurred with our recommendations and described corrective actions to resolve them. (*OSE-19164*)



Photo Courtesy NOAA/National Undersea Research Program

NOAA researchers preparing to drill into a coral reef to study climate over the past 20,000 years.



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 is dedicated to the stewardship of living marine resources through science-based conservation and management, and the promotion of healthy ecosystems.

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

Office of Oceanic and Atmospheric Research conducts environmental research, provides scientific information and research leadership, and transfers research into products and services to help NOAA meet the evolving economic, social, and environmental needs of the nation.

Office of Program Planning and Integration develops and coordinates NOAA's strategic plan, supports organization-wide planning activities, guides managers and employees on program and performance management, and integrates policy analyses with decision-making.

Data Buoy System Found to Have Declining Data Availability and Ineffective Contracting Practices

NWS' National Data Buoy Center (NDBC) operates three major buoy systems and a network of coastal marine observing stations that provide critical data on oceanic and atmospheric conditions for weather forecasters, oceanographers, commercial fishers, and others. The systems consist of (1) off-shore weather

buoys and Coastal Marine Automated Network, or C-MAN, stations; (2) Deep-Ocean Assessment and Reporting of Tsunami (DART) buoys; and (3) Tropical Atmosphere and Ocean (TAO) buoys. The latter two systems were developed and formerly operated by NOAA's Pacific Marine Environment Laboratory (PMEL).

In 2005, NDBC signed an indefinite-delivery indefinite-quantity contract with Science Applications International Corporation (SAIC) to operate and maintain



US Coast Guard photo by Tyler Johnson

A runaway NOAA weather buoy is recovered by the USCGC Ironwood after it drifted for six months in the Gulf of Alaska. The buoy will be repaired and returned to its station roughly 300 miles southwest of Kodiak Island.

the buoy networks. The contract has a \$500 million ceiling, with a 5-year base term and the possibility of five 1-year extensions. The U.S. Coast Guard provides the center with ship transit to the weather buoys for repair and maintenance, under the terms of a 1993 memorandum of understanding. NDBC leases privately owned vessels to service the DART buoys and uses a NOAA ship to service the TAO buoys.

We evaluated (1) the center's maintenance and repair operations for the buoys; (2) the adequacy and reliability of the buoy data; (3) the structure and administration of the support services contract; and (4) the transfer of the TAO and DART programs to NDBC. Our observations are as follows:

Declining availability of data from weather buoys

Though the center has historically met or exceeded its performance goals for the systems, weather buoy performance fell off sharply after August 2006. Data availability—the percentage of time that a typical buoy is operating properly and providing data—reached a 3-year low of 71.7 percent in April 2007—almost 19 percentage points below the 10-year average and more than 13 percentage points below the performance goal.

Unsuccessful repair calls

Frequent unsuccessful service visits complicate the center's efforts to maintain data availability. Coast Guard records indicated that between July 2005 and July 2007, 51 of 101 weather buoys received multiple service visits, with the average interval between visits only 107 days. Contractor error resulted in unsuccessful service outcomes for approximately 18 percent of the service visits in our sample. Factors such as incomplete records and inadequate training contributed to these errors. NDBC should work with its contractor to address these issues and reduce the number of unsuccessful service visits.

Unclear ship transit requirements

Both center and contractor personnel claimed that maintenance and repair efforts are further complicated by insufficient Coast Guard ship transport. But NDBC could not document this shortage or cite specific cases in which ship transit requests had been denied. And we found that the center was unsure of its exact ship transit needs because it had not clearly defined what service intervals are required to maintain data availability and had not fully utilized available Coast Guard resources.

We recommended that the center and its contractor (1) more clearly define required service schedules, (2) better coordinate ship transit needs with the Coast Guard, and (3) identify and prioritize its inventory deficiencies and take action to address them.

Deployment of untested equipment

We also found that NDBC deployed new oceanographic sensors without adequately testing them to ensure they work properly, and two of the three types deployed—current and salinity sensors—proved to be unreliable. Less than a third of these sensors were functioning at the time of our review, and NDBC will have to make adjustments to the 27 separate platforms on which the sensors were installed. In the future, NDBC should test new sensors on a limited number of buoys before widely deploying them.

Structure of contract incentives needs to be improved

In order to provide a performance incentive for the contractor, the center's contract with SAIC allows for the extension of the contract term beyond the 5-year base. However, the contract does not clearly define this provision and does not establish the prices of services to be delivered after the 5-year base term. NDBC should address the ambiguity and pricing issues. It should also obtain an opinion from the Department's Office of General Counsel on the permissibility of the extension or recompute the contract before the expiration of the base term.

The contract's questionable award-term provision is in part a reflection of the lack of departmental guidance on the use of award-term incentives. Commerce needs to prepare guidance for its contracting officers on award-term contracts and issue an administrative order clarifying the policies and procedures for its Acquisition Review Board.

The contract's fee scale does not promote superior performance: differences in award amounts for performance rated unsatisfactory through outstanding are insignificant. NDBC should adjust fees to maximize their effect on contractor performance, as permitted by the terms of the existing contract.

Inconsistent performance metrics

Performance metrics for the contractor often do not give appropriate weight to the center's core data availability goal and sometimes hold the contractor accountable for goals that differ from those of the center. NDBC has also not adequately disclosed all metrics and in some cases has been late in communicating them to the contractor. The center needs to ensure performance metrics are consistent with its own, and communicate them to the contractor in a timely manner.

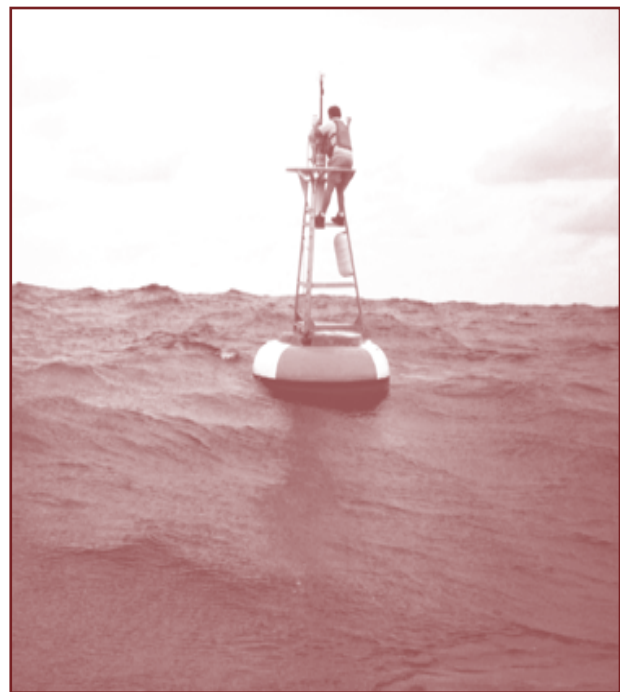
Difficulties transitioning DART and TAO buoy systems

NOAA transitioned the DART buoys from PMEL to the center over the course of 2 years (2001-03) and

began the TAO transition in 2005. Both transitions were problematic and NOAA oversight during the transitions was inadequate. In the case of DART, the center was not sufficiently prepared to fully support the buoys: NOAA had not clearly defined data collection requirements and the center did not have the technical capabilities to collect certain information. These problems, among other things, contributed to the loss of important observational data on the 2004 Sumatra tsunami.

For TAO, the center did not receive needed maintenance documentation and technical specifications, or enough funding to complete a required technology refresh. NOAA also did not provide adequate resources to support data collection and dual operations at both PMEL and NDBC during the transition period. In addition, NOAA researchers have been concerned about NDBC's ability and willingness to make needed system modifications to meet evolving data requirements.

Despite the transitions, PMEL has been planning enhancements for the two systems to meet various data



NOAA

A repair technician services a TAO buoy deep in the Pacific Ocean. NOAA maintains approximately 55 TAO buoys throughout the equatorial Pacific, enabling scientists to collect real-time, high-quality oceanographic and meteorological data for monitoring, forecasting, and understanding climate swings associated with El Niño and La Niña.

collection goals, and the center has similar projects under way as well. Although the two are aware of each other's research efforts, they have not worked together or consulted each other on the scope and objectives of their projects.

In future transitions, NOAA management should ensure that (1) the center develops a process to respond to emerging data requirements; (2) NOAA research organizations document the technical specifications and maintenance procedures of research systems; and (3) NOAA updates its administrative order on transitions to address issues arising from the DART and TAO transitions.

Finally, NOAA needs to foster improved internal communication and cooperation on research and development projects, such as those being conducted by PMEL and NDBC, to prevent duplication and ensure that individual design specifications consider the needs of all relevant organizations as appropriate.

Response from NOAA and the Department

NOAA concurred with all of our recommendations. Among other things, the National Data Buoy Center now develops site-specific field service plans, conducts pre-trip planning meetings, tracks the outcome of the contractor's buoy repair calls and has established a comprehensive training program for technicians. It also is documenting standard procedures for on-site visits, improving coordination and information-sharing with the Coast Guard, and implementing stronger inventory control processes. NOAA reports that it has improved its fee scale to provide the contractor with greater performance incentives, obtained a legal review of the contract term, and reevaluated performance metrics.

Regarding our two recommendations to the Department—that it issue guidance on the proper use of award-term incentives, and prepare a Departmental Administrative Order clarifying the role and authorities of the Commerce Acquisition Board—the Chief Financial Officer and Assistant Secretary for Administration reported that the Department is participating in an interagency task force to develop guidelines on

the use of incentives in government contracting and expects Commerce-specific guidance to be developed in tandem with this effort. He also noted the Department is refining the role and structure of its acquisition board in conjunction with developing a Department-level Investment Review Board, and a DAO addressing both is forthcoming. (IPE-18585)

Joint Enforcement Agreements Fall Short of Protection Potential

We assessed the efforts of the National Marine Fisheries Service's Office for Law Enforcement (OLE) to target living marine resource violations through the joint enforcement agreement (JEA) program. OLE relies on the U.S. Coast Guard and coastal state¹ marine enforcement agencies for help enforcing federal fisheries regulations within the 200 miles of U.S. coastline known as the U.S. Exclusive Economic Zone (EEZ). It uses joint enforcement agreements to transfer federal dollars to its state partners to fund their federal enforcement activities.

We had looked at the JEA program in 2003² and identified a number of needed improvements. We revisited the program during this semiannual period and noted some progress, but found several deficiencies that prevent NOAA from maximizing the benefits of its partnerships with the states. Our specific findings are as follows:

JEA Activities Need to Be More Closely Monitored

In our March 2003 report, we recommended that OLE divisions regularly verify state-reported enforcement activities and expenditures, and OLE headquarters conduct on-site reviews to confirm a partner's accomplishments and internal controls over program funds. OLE has since developed a Cooperative Enforcement Program Manual and initiated performance reviews. But the office has yet to (1) institute an adequate di-

¹ The term "state" also includes "territory" and "commonwealth."

² NMFS *Should Take a Number of Actions to Strengthen Fisheries Enforcement* (IPE-15154/March 2003).



NMF's Office Law Enforcement

Coast Guard and NOAA agents oversee crewmembers offloading their catch. Partnering with the Coast Guard and state enforcement agencies has enhanced NOAA's ability to enforce fisheries regulations through at-sea patrols and dockside inspections.

vision-level program that fully and regularly verifies state-reported activities or (2) conduct headquarters performance reviews of most JEA partners.

Division-level reviews

Most OLE managers we spoke with stated that the divisions lack resources to improve monitoring. However, five of the six division JEA coordinator positions are fully funded by the JEA program, yet none of the coordinators works full time on JEA activities. Because the program accounts for a substantial portion of OLE's federal fishery enforcement funding, we recommended that OLE ensure JEA coordinators dedicate 100 percent of their time to it. Additionally, OLE special agents in charge should regularly verify partner activities in order to tie program funding decisions to partner performance.

Headquarters reviews

OLE headquarters initiated independent reviews of program partners in September 2006, and to date has reviewed 10 of the 27 states receiving JEA funds. But it has reported its findings to only 6 of the 10, even though the remaining 4 reviews were completed more than a year ago. We found that OLE has no set time frame for reporting its results to the JEA partner upon completion of reviews.

We recommended that OLE develop a strategy for reviewing all partner programs that prioritizes the order in which it assesses them, verifies and evaluates a program's internal controls and accomplishments, and reports results to state JEA officials in a timely manner.

Use of Summary Settlements Is Limited and Loosely Managed

The summary settlement system was designed to process minor federal fishery violations efficiently by allowing enforcement officials in the field to issue tickets on the spot and giving violators the opportunity to pay a reduced penalty within a specified time period, in lieu of contesting an alleged violation and possibly going to court. If the party chooses not to pay the fine, the case is forwarded for prosecution to NOAA's Office of General Counsel for Enforcement and Litigation (GCEL). Because summary settlements are a type of civil penalty, law enforcement entities must receive authority to use them from GCEL.



NMF's Office Law Enforcement

A deputized fisheries enforcement agent patrols protected waters looking for fisheries violations.

Few partners authorized to use summary settlements

We found that only 3 of the 27 JEA partner states have authority to issue summary settlements. Some GCEL attorneys are resistant to extending this authority to more partners because they are concerned their caseloads will increase with an influx of unpaid or appealed tickets requiring litigation. But GCEL has not conducted any type of assessment to validate this concern.

OLE indicated that it plans to collaborate with GCEL and JEA partners to determine the most strategic use of summary settlement authority. We support this effort and recommended that OLE and GCEL develop specific criteria or guidelines for determining where and how the summary settlement system should be used.

No documented process for making and managing delegations of summary settlement authority

GCEL lacks formal policies and procedures governing how partners should receive and use summary settlement authority. As a result, we found that at least five states had been incorrectly told by OLE that they had summary settlement authority. OLE mistakenly believed that GCEL's delegation of authority automatically applied to JEA partners via their deputization to enforce federal fishery statutes. As our review was in progress, GCEL instructed OLE to advise the states to stop issuing summary settlements because they had not been delegated this authority.

For the three states that did receive delegation of authority, we found very limited documentation supporting the action—there is some electronic mail traffic between GCEL and OLE and OLE and state partners related to the two recent delegations, but no documentation for the remaining one.

We recommended that GCEL establish national policies and procedures for making and managing delegations of summary settlement authority. These should include requirements for maintaining written documentation of delegation decisions and providing written notification of these decisions to JEA partners.

NOAA Response

NOAA agreed with all of our recommendations and reported a series of actions it plans to take to implement them. (*IPE-19050*)

C&A Weaknesses Identified for NOAA Systems, But Some Improvements Were Made Through Continuous Monitoring

As part of our 2008 FISMA work, we evaluated the C&A process for four NOAA systems: the National Weather Service's Telecommunication Gateway and its International Satellite Communications System Data Acquisition and Delivery Network; the National Marine Fisheries Service's Science and Technology System, and the Satellite Environmental Processing System operated by the National Environmental Satellite, Data, and Information Service (NESDIS). We also tested selected security controls on the NWS Telecommunication Gateway and the NMFS Science and Technology System.

As we had done at BEA, we revisited three NOAA systems—the Gateway, International Satellite Communications, and Science and Satellite Technology systems—after our C&A work had concluded to determine whether continuous monitoring was in fact having the desired effect. In the case of Gateway, we found that NOAA had recertified the system and that the control assessments we reviewed were rigorous and supported by adequate evidence. For the International Satellite system, NOAA provided evidence of improvements to the security control assessments that occurred as part of its continuous monitoring program. We found continuous monitoring for the Science and Technology system to be ineffective.

The results of our FISMA work at NOAA are summarized below.

National Weather Service's Gateway System Certification Assessments Were Deficient, But NOAA Took Action to Improve Them

The gateway system collects, processes, and disseminates national and international meteorological data and products in real time. The system interconnects with numerous other systems worldwide, and its data is used by other government agencies, the private sector, and the general public.

We found that NWS began certifying the system before it had adequately defined security controls in the system security plan or gotten formal review and approval of the plan, resulting in an ineffective C&A process. In fact, the plan was approved on the same date as the system was accredited, which means during the course of the certification, certifiers lacked the information they needed to effectively assess controls: the plan they were using contained incomplete specifications for security control enhancements and parameters, and it incorrectly identified a number of physical and environmental security controls.

In addition, we found that NWS did not test secure configuration settings for any system-related IT products (e.g., servers, desktops, routers, switches) and in some cases had not even defined these settings. We also found that certification assessments were incomplete and flawed—the C&A documentation lacked evidence of security control testing on several system components and applications. In some cases, the assessment erroneously indicated that certain procedural steps for control assessments were related to NOAA common controls (controls applicable to a number of systems). In others, test results were inappropriately based on interviews and document reviews or other improper procedures, contained inconsistent evidence, or did not describe vulnerabilities discovered.

Finally, in our own evaluation of a set of system components we found significant control weaknesses not identified in the NWS security certification.

We recommended that NOAA, among other things, promptly add the deficiencies we identified to the



system's plan of action and milestones and remediate them in a timely manner, as well as ensure system security plans are approved prior to certification; secure configurations are defined and implemented on all IT products; and assessments test controls on all applicable system components according to applicable procedures.

NOAA Response

NOAA agreed with all but one of our findings, noting that the system security plan had been favorably reviewed by the NWS information security officer and approving official prior to certification, though not signed. NOAA described actions that are fully responsive to our recommendations. (OSE-19000)

Significant Weaknesses Evident in C&A for International Satellite System, But Improvements Made Through Continuous Monitoring

The International Satellite Communications System Data Acquisition and Delivery Network is a complex wide area and satellite network designed to distribute critical weather data to remote sites across the globe. The network consists of three earth stations, four contractor operations centers, and one NOAA location. A contractor has owned and operated the system on behalf of NOAA since 2003, but it was granted its first authorization to operate in March 2007.

A September 2006 OIG report, *Additional Steps Are Necessary to Provide Better Oversight of Contractor Infor-*

What Is a Certification and Accreditation Package?

Security certification and accreditation packages contain three elements, which form the basis of an authorizing official's decision to accredit a system.

1. The *system security plan* describes the system, the requirements for security controls, and the details of how the requirements are being met. The security plan provides a basis for assessing security controls also includes other documents such as the system risk assessment and contingency plan, per Department policy.
2. The *security assessment report* presents the results of the security assessment and recommendations for correcting control deficiencies or mitigating identified vulnerabilities. This report is prepared by the certification agent.
3. The *plan of action & milestones* is based on the results of the security assessment. It documents actions taken or planned to address remaining vulnerabilities in the system.

mation Security (Report No. OSE-18028), found that NOAA was not applying FISMA and Commerce IT security requirements to some of its contractor-managed information technology systems. So NOAA subsequently decided the international satellite system should meet those requirements and initiated the certification and accreditation process that resulted in the 2007 authorization. NOAA's service contract for the system did not include the Department-mandated IT security clauses requiring a contractor's compliance with Commerce and FISMA requirements. NOAA told us that its contractor was initially resistant to adding these clauses because of cost and liability concerns. As a result, the agency devised an alternative contractual agreement to allow the contractor to conduct the C&A, with agreement by both parties to subsequently add the IT security clauses and jointly manage the information system security. NOAA officials told us they viewed the C&A as an initial audit of the system, and as an opportunity for the contractor to understand FISMA requirements.

In performing the initial certification and accreditation, NOAA and the contractor were essentially "starting from scratch" in meeting FISMA requirements: the system had no defined accreditation boundary—that is, no inventory of all system resources to be addressed in the C&A. There was also no security plan, and no specified security requirements and control implementations. Secure configuration baselines were not defined for IT products.

Our evaluation found that key C&A planning activities were not adequate or appropriate: though NOAA had defined a security boundary, it was incomplete and in some cases inaccurate. System descriptions were deficient and remained so at the time of our review—more than a year after the system was authorized to operate. We also found that the same individuals both developed the security plan and assessed security controls, contrary to NIST requirements that these duties be separated.

None of the significant deficiencies identified during certification were properly listed on a plan of action and milestones. Even after the plan was developed, NOAA did not submit it for more than a year after authorizing the system to operate, which prevented both the Department and OMB from properly tracking the deficiencies' resolution in the interim.

Finally, letters justifying the accreditation decision incorrectly asserted that security controls were in place and a timetable for addressing vulnerabilities had been established.

We recommended that NOAA properly define the accreditation boundary and security controls in the system security plan, the authorizing official approve the system security plan in accordance with NIST guidance, and the certification agent not be involved in security planning activities. We also recommended that NOAA set completion dates for resolving weaknesses and submit the system POA&M to the Department in accordance with policy.

NOAA Response

NOAA officials generally agreed with our findings and recommendations and described corrective actions to address them. (OSE-19166)

Widespread Weaknesses in C&A for NMFS Science and Technology System

The Science and Technology System processes complex scientific and general data for the National Marine Fisheries Service, and supports an array of agency operations and research—data and information management, fisheries surveys, and stock assessments, to name a few. NMFS Science and Technology staff manages the system, but various information owners within NMFS manage the system’s applications and are responsible for related security controls.

Our FISMA review of this system identified widespread weaknesses in the C&A process:

- The security plan did not provide an adequate basis for certification and accreditation.
- The certification team did not adequately assess controls.
- The system plan of action and milestones did not report known vulnerabilities and was not submitted to the Department as required by policy.

Our own assessment of certain system components found weaknesses in a number of operational and technical controls requiring remediation.

We concluded that the authorizing official lacked sufficient information about system vulnerabilities to make a credible, risk-based decision on whether to accredit the system.

We advised NOAA to improve security planning to include all information required by the Department’s IT security policy and NIST guidance; ensure that the system’s security certification is based on a rigorous assessment of controls; report known vulnerabilities—including those we identified in our own testing—on the system plan of action and milestones and submit the plan to the Department OCIO.

NOAA Response

NOAA generally concurred with our findings and recommendations, noting changes to the NMFS IT

Additional Commerce Requirements

Commerce’s IT Security Program Policy and Minimum Implementation Standards requires that C&A documentation contain supporting evidence of the adequacy of the security assessment. Two important components of this documentation are:

1. the *certification test plan*, which documents the scope and procedures for testing (assessing) the system’s ability to meet control requirements; and
2. the *certification test results*, which is the raw data collected during the assessment.

security program in the months since the system’s accreditation may have addressed many of our concerns. The bureau also indicated that it is working with the Department to deploy the Cyber Security Assessment and Management (CSAM) tool that it believes will further address our recommendations.

However, our check of subsequent security materials and activities indicate that the revised NMFS security program still falls short of meeting minimum security requirements—a situation confirmed by the results of continuous monitoring. While we do believe CSAM will enable NOAA to better comply with FISMA and Department IT security policy requirements, we remain concerned that NOAA management is giving insufficient attention to IT security at NMFS. (OSE-19165)

NESDIS System Did Not Comply with Department IT Security Requirements

The Satellite Environmental Processing System (SATEPS) collects, processes, stores, and disseminates global weather satellite data for foreign and domestic users.

We selected SATEPS for review because according to the Department’s information system inventory, it had been recently accredited, with an authorization

learned this information was incorrect. SATEPS was scheduled to be decommissioned prior to September 22, 2007, when its last authorization to operate would have expired. But decommissioning was delayed, so NESDIS extended the original authorization rather than initiate a new certification and accreditation process.

Our evaluation found that SATEPS operated for at least 2 years with significant deviations from mandatory security requirements—most notably, the system’s security plan had not been updated since June 2005 and a number of required security controls were not in place. NESDIS did not seek waivers from the Department to forgo these requirements, even though Commerce IT security policy obligates agencies to do so. Despite significant deficiencies with SATEPS’ security controls, we found the authorizing official received sufficient information to make a credible, risk-based decision to extend SATEPS authorization to operate.

SATEPS was finally decommissioned in February 2008. In light of the security lapses the agency permitted while the system was active, we recommended that NOAA officials give NESDIS systems appropriate management attention and ensure all systems are operating in full compliance with the Department’s IT security policy.

NOAA Response

NOAA officials generally agreed with our findings and recommendations, noting the deployment of the Cyber Security Assessment and Management tool will play a significant part in addressing our recommendations. (*OSE-19167*)



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Comprehensive Operating Plan Needed for Overseas Intellectual Property Rights Attaché Program

Theft of intellectual property rights—copyrights, trademarks, patents, industrial designs, and trade secrets—costs the United States hundreds of billions of dollars each year and hundreds of thousands of jobs. It affects manufacturing, technology, pharmaceuticals, and numerous other industries.

The United States Patent and Trademark Office promotes intellectual property rights protection and enforcement domestically and abroad by conducting outreach and training activities, working to secure strong international agreements on intellectual property rights, and encouraging U.S. trading partners to strictly enforce these agreements and protections.

In 2005, USPTO began posting attaches at U.S. embassies to provide legal and technical expertise on intellectual property rights issues. Attaches are currently posted in Brazil, China, Egypt, India, Russia, and Thailand.

We evaluated the attaché program to learn whether its objectives are adequate and how the attachés work with other government agencies. We also looked at USPTO's attaché recruitment process, training, and terms of appointment, as well as the agency's method of placing attachés in posts.

We found the attachés are generally coordinating their activities with other U.S. government agencies and have good relationships with their U.S. mission counterparts and with host government officials. However, the roles and responsibilities of the attachés in relation to the International Trade Administration's Commercial Service and the U.S. Department of State need to be better defined. In addition, guidelines and criteria for program expansion need to be addressed, as do attaché training and program continuity.

We recommended USPTO develop and implement a comprehensive operating plan for the attaché program in consultation with relevant U.S. government agencies to better integrate attachés in their respective U.S. overseas missions and help them perform their duties effectively. The plan should cover everything from recruiting candidates to ensuring intellectual property rights coverage and continuity when attachés



USPTO

Secretary Gutierrez poses with USPTO's overseas intellectual property rights attaches at USPTO headquarters in December 2007. The group was gathered for a week-long consultation with USPTO colleagues, members of industry, and other U.S. government agencies.

transition to other posts. USPTO agreed with our recommendation and told us it expects to have a plan in place by the first quarter of FY 2009. (IPE-19044)

FISMA Reviews Identify Significant Weaknesses in Patent Systems' C&A Process

Security Plan, Assessments Lacking in Landon IP System C&A

We evaluated the Landon IP information system, which is owned and operated by a contractor. The Landon IP system supports the USPTO international patent application process under the Patent Cooperation Treaty (PCT). The PCT provides a unified procedure for filing patent applications to protect inventions in each of the states party to the treaty. Landon IP analysts conduct searches on applications received from USPTO via a secure communications channel, develop opinion papers on the invention, and return the papers to USPTO via the same secure communications channel.

Prior to our evaluation, USPTO had a consultant independently assess the system's C&A documentation. The consultant reported significant deficiencies with the system security plan, contingency plan, and control assessments. But these weaknesses were not

included in the plan of action and milestones we received for review.

Our evaluation identified a number of additional weaknesses, for the most part pertaining to assessment procedures that USPTO either omitted or performed inadequately. For example, it assessed components that were not within the system's accreditation boundary because system diagrams and component inventories did not match; did not evaluate the appropriateness of access control procedures, which we found to be lacking in substance; did not assess whether system components are configured to disable inactive accounts automatically; and did not follow proper procedures for assessing remote access controls.

The contract staff operating the Landon IP system explained that system diagrams and inventories did not match at the time of certification testing because the system boundary had not been finalized. We recommended that USPTO (1) define accreditation boundaries before certification begins, and (2) add the deficiencies identified by both the consultant and OIG to the system's plan of action and milestones.

USPTO Response

USPTO indicated its intent to comply with our recommendations, but took exception to our finding that certification testing occurred before the accreditation boundary was finalized. The agency asserted that the boundary had been finalized prior to certification testing, and provided the date. We do not dispute the document may have been approved, but it clearly did not reflect a final consensus. For example, the certification team assessed controls on the system's web site, which was not identified in the approved boundary definition document. During our review, both USPTO personnel and Landon IP staff informed us that discussions about the system's boundary were ongoing during testing, and the web site had been initially included in the boundary but was later removed. (OSE-19367)

Security Plan, Common Controls Weaknesses Among Problems Noted in C&A for Enterprise Remote Access System

The Enterprise Remote Access (ERA) System enables USPTO personnel to perform their official duties remotely from alternative worksites supporting USPTO telework programs and initiatives. ERA facilitates the secure remote access of communications, protective services, and network infrastructure support for all USPTO applications. ERA system components were certified and accredited under the USPTO Network Perimeter system in FY 2007. However, due to the large size of the USPTO infrastructure, management decided to restructure the accreditation boundary of the Network Perimeter system into more manageable components. USPTO's chief information officer authorized ERA to operate on May 22, 2008.

Our review revealed the following:

- The system security plan needs improvement—it did not fully define the accreditation boundary or adequately describe certain controls.
- The common controls the bureau selected did not meet the system's minimum security requirements.
- A number of technical controls were not assessed. Numerous others were not assessed according to required procedures, yet they were reported as fully meeting requirements.
- The plan of action and milestones did not give completion dates for resolving deficiencies.

We concluded the C&A process did not give the authorizing official the necessary information to make a credible, risk-based accreditation decision. USPTO needs to ensure that all required system-specific and common controls are implemented and must improve control assessments to verify that controls are implemented correctly, operating as intended, and meeting security requirements, and must ensure the certification team has the access it needs to thoroughly assess controls.

USPTO Response

USPTO generally concurred with our recommendations but disagreed with our finding that the security plan did not fully define the accreditation boundary or test controls on certain components. The bureau contended that the boundary was accurately defined and that the system owner does not manage the component we stated should have been included. The component, according to USPTO, was therefore not subject to control assessment.

However, we note that the component was included in the security plan's desktop descriptions and was referenced as within the boundary in our discussions with USPTO officials. Whether the component is or is not within the boundary, the discrepancy supports our finding that the security plan needs improvement, to include precise definition of the system boundary, which will then dictate which components and associated controls require testing. We learned that the ERA system accreditation boundary is continuing to evolve and USPTO is aware of the need to clearly define boundaries in order to adequately plan and assess controls. (*OSE-19368*)

USPTO's Privacy Impact Assessment Process Met Federal Requirements

As part of our FISMA work, we assessed USPTO's privacy impact assessment process. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments of information systems and collections containing personally identifiable information and, in general, to make these assessments publicly available.

We found that USPTO has implemented an effective process for conducting privacy impact assessments, consistent with the E-Government Act and OMB guidance. Since we made no recommendations and no actions were required of USPTO, we did not issue a report but included the results in our annual FISMA report to OMB.



Photo Courtesy Commerce Photographic Services

Commerce Law Library



DEPARTMENT-WIDE MANAGEMENT

The United States Department of Commerce creates the conditions for economic growth and opportunity by promoting innovation, entrepreneurship, competitiveness, and stewardship. The Department has three stated 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 2006 Earmarks Match Mission

In August 2006, we received a request from Senator Tom Coburn-R, OK, then-Chairman of the Subcommittee on Federal Financial Management, Government Information, and International Security, to conduct an analysis of the Department's congressional earmarks. Senator Coburn asked that we determine (1) the total number and cost of congressional earmarks within the programs monitored by OIG, including the cost of each earmark itself and related costs such as staff time and administration; (2) the specific oversight conducted on earmarks and how the oversight compares to that conducted on other expenditures such as grants and contracts, and (3) the overall impact of earmarks on advancing the primary mission and goals of the Department.

We identified 327 earmarks totaling \$798.8 million in FY 2006, or 9.6 percent of the total Commerce budget of \$8.3 billion for that year—the most recent year for

which data was available. More than 90 percent of the number of earmarks in Commerce went to NOAA, which had 298 earmarks totaling \$594.5 million (\$459 million of which was for NOAA projects not included in the President's budget).

Costs of Administering Earmarks Not Separated

Commerce bureaus do not account for staff time and costs of administration for earmarks separately from other costs. Bureaus have a variety of practices for charging fees for grant administration for earmarks. NOAA line offices may charge up to 5 percent of the earmark pursuant to the Department's budget reprogramming authority, which was capped at \$750,000 in FY 2006. ITA also charges for grant oversight and administration, usually between 1.5 to 3 percent of an earmark, totaling \$355,402 in FY 2006. NIST does not charge earmarks a fee for grant administration. Census, USPTO and the departmental management category do not have earmarked grants.

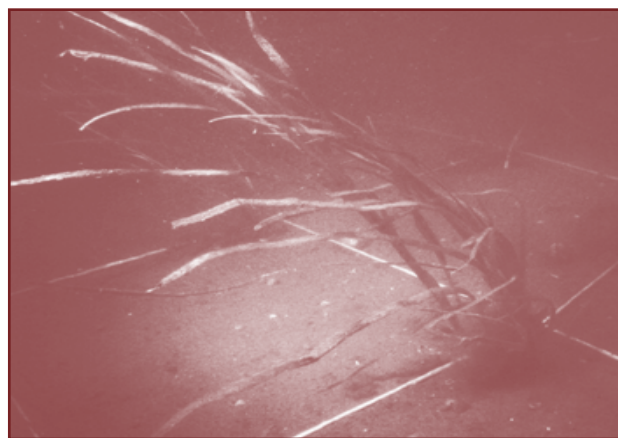
Oversight of Earmarks Is the Same

We found oversight of FY 2006 earmarked grants and contracts is the same as the oversight for non-earmarked grants and contracts. Applications are required, and recipients have to follow the same rules as recipients of other types of awards.

Earmarks Are Consistent with Department Goals and Mission

Commerce bureau officials we interviewed were in agreement that all of the FY 2006 earmarks were consistent with the Department's mission and strategic goals. Our review of a nonstatistical sample of 32 earmarked grants from three Commerce bureaus (ITA, NIST and NOAA) found that all were consistent with the mission of the Department.

We did not make recommendations because the pur-



NOAA

NOAA is using earmarked funds to help restore eelgrass in Narragansett Bay, RI, and the shellfish that depend on this underwater vegetation. Our review found that—like this NOAA project—Commerce earmarks support mission activities.

pose of this review was to conduct an independent analysis of Commerce's congressional earmarks for FY 2006. We gave bureau officials the opportunity to review the report and provide informal comments prior to its release. Bureau officials agreed with our report, and we incorporated their suggestions into the report. (DEN-19021)

Privacy Impact Assessments Are Generally Meeting Federal Requirements But Must Be Updated to Reflect Recent Commerce Policy Changes

Federal agencies obtain and maintain significant amounts of personally identifiable information about individuals, which must be protected. The E-Government Act of 2002 requires agencies to conduct privacy impact assessments of information systems and collections containing personally identifiable information and, in general, to make these assessments publicly available. The act also requires agencies to post their privacy policies on their web sites in a computer-readable format. The Department's IT privacy policy defines the responsibilities Commerce operating units have for conducting impact assessments and posting them along with web privacy policies on their web sites.

OMB requires offices of inspectors general to examine the processes agencies use to conduct these assessments as part of their reporting under the Federal Information Security Management Act. We evaluated whether the Department's privacy impact assessment process adheres to existing policy, guidance, and standards. We also evaluated the Department's processes for ensuring ongoing compliance with web privacy policies and computer-readability requirements.

Commerce Policy Needs to Be Updated

In a December 18, 2007, memorandum to all chief information officers, entitled Data Extract Log and Verify Requirement, the Department's CIO required operating units to take the following actions by March 28, 2008:

- Review and update all existing privacy impact assessments, specifically describing how the log and verify requirement of OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, has been implemented for the system.

- Develop privacy impact assessments for all databases containing investigative, law enforcement, and human resources information even if they were previously exempt.

Although the stated purpose of the memorandum was to document the implementation of OMB's data extract log and verify requirement, it effectively changed the privacy impact assessment exemption for legacy and operational systems, as well as for systems that contain information only about federal employees, to require that all Commerce systems containing personally identifiable information be assessed.

We also found the Department had requested that privacy impact assessments document whether the records collected are being retained and, if so, to include the specified retention schedule.

We recommended the Department update its IT privacy policy to incorporate these new requirements for privacy impact assessments, and revise its IT Security Policy and Minimum Implementation Standards to reference the IT privacy policy as guidance for conducting assessments.

Some Privacy Impact Assessments Are Incomplete

We also found some impact assessments do not address all required elements. We reviewed 20 assessments and found they generally met the intent of OMB's guidance. However, 4 did not sufficiently address elements required by OMB and 14 did not include sufficient information for certain elements required by Department policy—such as the reason the assessment was conducted or the law or regulation authorizing the information be collected and maintained. We recommended the Department clarify certain sections of its IT privacy policy, consider developing additional guidance on the level of detail to be provided for each assessment element, and approve only those impact assessments that contain all required elements.

Scope of Compliance Check for Web Privacy Policy Is Too Limited

The Department's web policy, *Privacy of Visitors to DOC Web Sites*, requires all Commerce sites to have computer-readable privacy policy statements that describe in plain language how the site collects and handles personal information; how users can consent to the policy; how sites that have interactions with children handle getting parental consent, and other issues.

Each year, operating units must certify to the Department that their sites comply with the Department's web policy. Those that do not comply must explain why and set a target date for eliminating the deficiency.

Department CIO staff validate reported results by evaluating Commerce's 21 "major" web sites—which include the Commerce homepage, six NOAA sites, and homepages for several other operating units. However, the Department's FY 2007 annual compliance report identified 842 Commerce web sites because so many operating units—like NOAA—have multiple sites. To ensure compliance with its web policy requirement, the Department should validate a larger, more representative number of Commerce web sites each year. We also found that the evaluation process did not validate the computer readability of the web privacy policies to ensure users can be alerted automatically when posted web site policies do not match their privacy preference setting.

Department Response

The Department's Chief Information Officer concurred with all of our recommendations. (OSE-19047)

Commerce Needs to Implement New Contracting Policies

During this semiannual period, we advised the Department that contracting officers had not been notified of their new responsibilities for handling certain contract-related duties that were formerly performed by the Small Business Administration (SBA). The new responsibilities are pursuant to a June 2007 partnership agreement on the 8(a) Business Development Program between Commerce and SBA. The 8(a) program, authorized by the Small Business Act, promotes business development by giving preference to selected firms owned by socially and economically disadvantaged individuals including Alaska Native Corporations. One such preference, for example, makes it easier to award some sole-source contracts to these companies.

We also found the Department had not implemented OMB-mandated certification programs for program and project managers and for contracting officer technical representatives. The Department’s existing program and project managers should have been certified by April 25, 2008. Certification for technical representatives was required beginning in May. (Commerce had established a certification program for technical representatives in 2004, but it did not meet OMB’s new requirements.)

Commerce released draft certification policies in late May 2008, which were finalized in late June. Staff in the Office of Acquisition Management told us they were actively working to implement the new policies.

We recommended the Department immediately inform contracting officers of their new oversight responsibilities for 8(a) contracts and promptly begin implementing training and certification programs for procurement professionals to meet OMB requirements. (IPE-19045)

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 193 audit reports during this semiannual period to determine whether they contained any audit findings related to Department programs. For 97 of these reports, the Department acts as oversight agency and monitors the audited entity’s compliance with OMB Circular A-133 or NIST’s program-specific reporting requirements. The other 96 reports are from entities for which other federal agencies have oversight responsibility. We identified 13 with findings related to the Department.

| Report Category | OMB A-133 Audits | ATP-Program-Specifics Audits | Total |
|------------------------------|------------------|------------------------------|-------|
| Pending (April 1, 2008) | 25 | 5 | 30 |
| Received | 164 | 59 | 223 |
| Examined | 147 | 46 | 193 |
| Pending (September 30, 2008) | 42 | 18 | 60 |

The following table shows a breakdown by bureau of approximately \$716 million in Commerce funds audited.

| Bureau | Funds |
|--------------|-----------------------|
| EDA | \$ 183,297,299 |
| ITA | 303,908 |
| NIST* | 70,913,300 |
| NOAA | 77,271,369 |
| NTIA | 752,684 |
| Multiagency | 383,028,411 |
| Total | \$ 715,566,971 |

* Includes \$67,178,707 in ATP program-specific audits.

We identified a total of \$3,243,336 in federal questioned costs and \$203,292 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 13 reports with Commerce findings are listed in Appendix B-1. (*Regional Offices of Audits*)



Photo Courtesy Commerce Photographic Service

US flag draped outside Commerce headquarters.



OFFICE OF INSPECTOR GENERAL

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.

Office of Investigations

Former Research Scientist Convicted of ATP Grant Fraud

As detailed in our September 2007 Semiannual Report (page 50), in June 2007, the recipient of a \$2 million NIST Advanced Technology Program award was indicted for program fraud after an OIG investigation found that hundreds of thousands of dollars from the grant had been diverted to the defendant's personal use. On June 12, 2008, the scientist was convicted in Federal District Court for the Southern District of New York of intentionally misapplying approximately \$500,000 of the grant funds to pay for numerous personal expenses, including rent, home renovations, cleaning services for his condominium, restaurant meals, and miscellaneous household items.

This conviction was the result of a collaborative effort between OIG's Atlanta Regional Office of Audits and the Office of Investigations that began in 2003, when audits of the recipient identified overstated project expenses and inappropriate costs of \$547,425 charged against the grant. The auditors and investigators worked together to analyze the recipient's bank-

ing activities to determine how the federal funds were being used. The findings of this analysis provided key evidence in the trial.

The scientist faces a maximum sentence of 10 years in prison and a maximum fine of \$250,000 or twice the gross pecuniary loss or gain derived from the offense. Sentencing is scheduled for October 2008. (*Atlanta Field Office of Investigations and Atlanta Regional Office of Audits*)

Workers' Compensation Investigation Leads to Recovery of Benefits

On June 16, 2008, a former employee of the Minority Business Development Agency was ordered to repay more than \$180,000 she had received in disability benefits. An OIG investigation revealed that she had failed to report outside earnings on annual certifications filed over a 6-year period while simultaneously receiving the federal disability payments.

The individual had been on disability since June 2002 following a claim that she had sustained on-the-job injuries in a fall while traveling on government business. Her monthly benefits were approximately \$3,500. The OIG investigation found that the individual had failed



to report rental income she was concurrently receiving from September 2003 through February 2008 as owner and landlord of a property investment and management company. (*Atlanta Field Office*)

NOAA Grantee Indicted, Pleads Guilty to Theft of Federal Funds

On September 24, 2008, a NOAA grantee pled guilty to one count of theft following his indictment by a Federal Grand Jury in the District of Hawaii. An OIG investigation revealed that the grantee had spent \$60,000 of the \$109,886 award on drugs, clothing, a Rolex watch, and other items, as well as on hotel accommodations. The NOAA grant was intended to train 40 native Hawaiian people in fishing techniques. Sentencing is scheduled for January 2009. (*Atlanta Field Office*)

NWS Employee Pleads Guilty to Credit Card Theft

On September 12, 2008, a National Weather Service (NWS) employee pled guilty to one count of theft of property for charging more than \$4,400 in personal

purchases to a credit card she had falsely opened in the name of the NWS. An OIG investigation found that in 2006, the employee opened the account online and over a 4-week period purchased DVD players, an MP3 player, two laptop computers, and other items totaling \$4,423.92. NWS discovered the theft after the employee defaulted on payments and a collections agency contacted NWS management. The employee was sentenced to 5 years probation and ordered to pay restitution of \$4,006.05 (the current account balance) and complete 120 hours of community service. (*Denver Resident Office*)

ITA Intern Sentenced for Credit Card Theft

As reported in our March 2008 Semiannual Report (page 25), a former intern of the International Trade Administration was convicted of felony credit card fraud in Fairfax County, Virginia, Circuit Court, after a joint OIG/Fairfax County Police investigation discovered the intern had used his position to obtain government credit card information on various high-ranking Commerce officials including the Secretary of Commerce. As part of his official duties, the intern prepared clearances for Commerce trade missions and had access to account numbers and expiration dates for government travel credit cards, as well as full names, dates and places of birth, and passport information. The intern used the credit card information to purchase thousands of dollars worth of tickets via an Internet travel site. He was sentenced on July 18, 2008 to 2 years in prison, 2 years probation, and ordered to pay more than \$52,000 in restitution. (*Silver Spring Resident Office*)

Former NIST Employee Pleads Guilty, Forfeits Assets in Major Theft Scheme

On August 8, 2008, a former NIST engineering technician and coordinator of the agency's Charpy impact testing program, pled guilty in U.S. District Court for the District of Colorado to one count of theft of government property and one count of asset forfeiture related to his work with the Charpy program. This program evaluates the integrity of industrial machines used to test the strength of structural steel for construction.

An OIG investigation revealed the individual—while coordinator of the program—had stolen 900 pounds of government-owned steel test specimens valued in excess of \$500,000 and removed a copy of the program’s customer database, which contained proprietary information. He diverted the stolen property to a company he had formed for the purpose of selling steel test specimens. For a year, while still employed at NIST, he operated the business and sold specimens identical to those produced by NIST. He retired from the agency in 2003 and continued operating the business until March 2006, when OIG investigators executed a search warrant at his residence, recovering some of the stolen property and other evidence including financial records and computer files.

Forensic analysis of the financial and computer data revealed the defendant had realized economic benefits of between \$400,000 and \$1 million from the stolen property. He was ordered to forfeit all assets derived from or traceable to the proceeds generated from the stolen steel. The approximate value of the property to be forfeited is between \$900,000 and \$1,000,000. Sentencing is scheduled for December 2008. (*Denver Resident Office*)

Commerce Employee Arrested for Metrochek Fraud

OIG special agents arrested an Office of the Secretary employee for first-degree theft after a joint investigation with Washington, D.C., Metropolitan Police disclosed that the employee received \$1,950 in transit subsidy benefits while assigned a parking space at the Commerce headquarters building, and gave the benefits to a relative. Between October 2004 and March 2007, the employee certified at quarterly benefits distributions that she had not been issued a federal parking permit and would not transfer the benefits to anyone else. A hearing in Superior Court of the District of Columbia is scheduled for October 2008. (*Washington Field Office*)

Convictions, Restitution, and Jail Terms Mount in Massive Telemarketing Fraud Case

An ongoing joint Commerce OIG, Immigration and

Customs Enforcement, Postal Inspection Service investigation of an international telemarketing fraud scheme detailed in our September 2007 and March 2008 Semiannual Reports continued to produce convictions and orders for significant restitution and jail time during this reporting period.

The scheme was perpetrated by callers identifying themselves as employees of the Commerce Department and other federal agencies, who told victims they had won huge cash prizes in a national lottery. They asked “winners” to pay insurance and customs fees and to wire funds to guarantee prize delivery. Investigators have so far identified transfers of more than \$30 million from U.S. citizens to Costa Rica, where the scheme was based, but the worldwide total could top \$1 billion.

During this semiannual period, 14 defendants were sentenced and four others convicted on conspiracy and wire fraud charges. They all face prison terms ranging from 3 to 50 years. In addition one more individual was arrested and two indicted. Total restitution ordered thus far exceeds \$100 million.

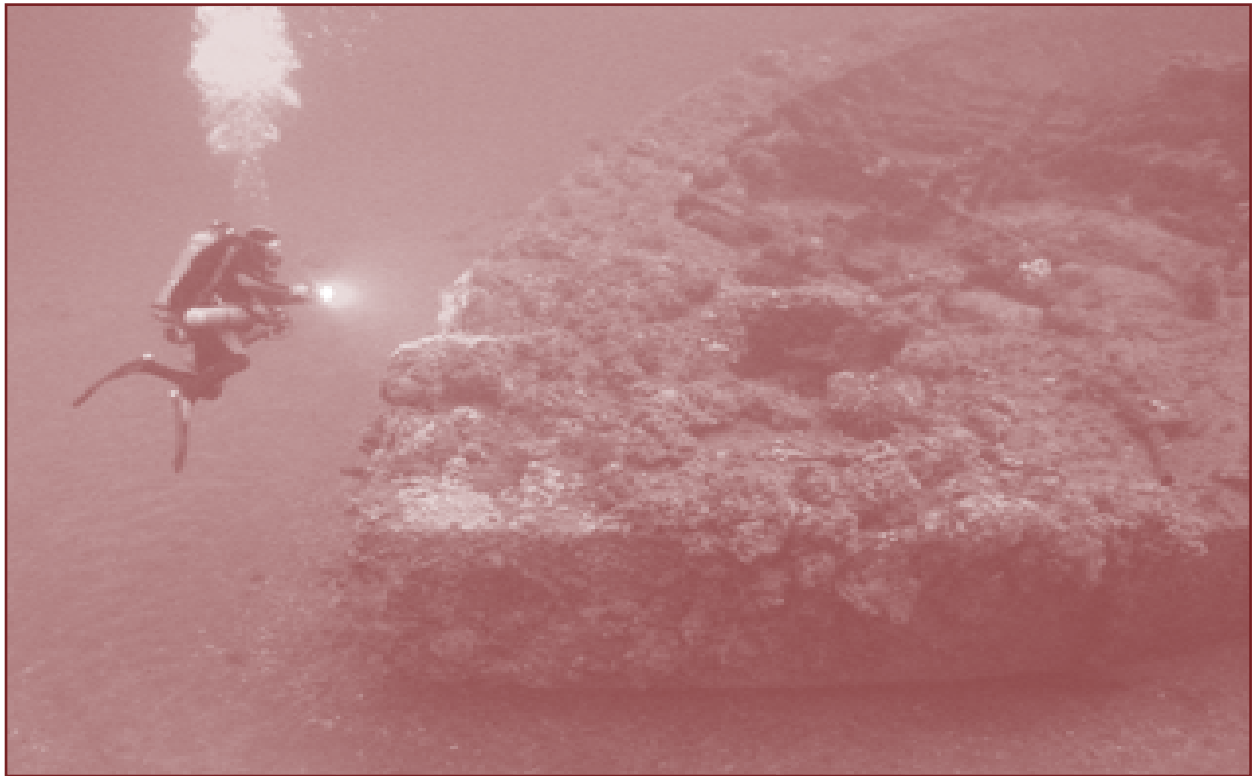
Over the past 5 years, this investigation has netted nearly 40 arrests and 30 convictions of Americans and Canadians involved in plots to defraud U.S. citizens. The investigation is an integral part of the Department of Justice’s Operation Global Con, a massive international fraud investigation involving nearly 3 million victims. (*Atlanta Field Office*)

Other Activities

The Inspector General Testifies on Reauthorization of National Marine Sanctuaries Act and Economic Development Administration

National Marine Sanctuaries Act

On June 18, 2008, the Inspector General testified before the House Subcommittee on Fisheries, Wildlife and Oceans regarding OIG’s oversight of the Nation-



NOAA

A Navy diver examines the bow of the Civil War ironclad USS Monitor. The Monitor was designated the nation's first national marine sanctuary in 1975.

al Marine Sanctuary Program as Congress deliberated reauthorizing the legislation that created the sanctuary system. The last reauthorization was in 2000.

Mr. Zinser described the sanctuary program as effectively protecting marine resources in the 13 marine sanctuaries and one marine national monument. He told the subcommittee that a 2008 OIG evaluation found the program is meeting objectives despite major challenges, which include (1) managing underwater areas that are far-reaching and geographically dispersed—encompassing more than 158,000 square miles of ocean and Great Lakes marine habitats; and (2) balancing the protection and conservation of resources with vital commercial interests.

In addition, the Inspector General noted, assessments by OMB and the National Academy of Public Administration found the program to be well managed and effective.

Mr. Zinser added that many stakeholders view the sanctuary program favorably, and would like to see it expand. But a threshold question for the reauthoriza-

tion is whether the program is ready for expansion. The IG stated that NOAA needs to engage in a transparent process to develop a list of potential sites for future designation and determine the factors, criteria, and resource needs for adding sanctuaries. He gave the subcommittee three recommendations for consideration in reauthorizing the act:

1. Giving the Secretary of Commerce the flexibility to establish management plan time frame requirements to reflect variations in the complexity and circumstances of the sanctuaries, instead of the 5-year time frame that all sites must currently meet, regardless of their size.
2. Giving the Secretary the same authority for managing marine monuments as he now has for managing the sanctuaries, such as assessing civil penalties for violations, recovering damages for injuries to sanctuary resources, and creating community-based advisory councils.
3. Establishing a separate title within the act that specifies protection of maritime heritage resources to strengthen the act's current empha-

sis on preserving maritime historic and cultural resources.

Beyond reauthorization, Mr. Zinser briefly mentioned the need for stronger enforcement of sanctuary regulations and noted that among other things, NOAA should finalize a national plan for sanctuary enforcement; and consider making greater use of summary settlement schedules, which set fixed fine amounts for misdemeanors and allow both federal and state enforcement officers to issue tickets on the spot. (View the complete testimony at www.oig.doc.gov.)

Economic Development Administration Reauthorization

On September 9, Mr. Zinser testified before the Senate Subcommittee on Transportation and Infrastructure on the 2008 reauthorization of Commerce's Economic Development Administration.

Mr. Zinser described EDA's grants programs and funding, which totaled approximately \$250 million in FY 2007, and OIG's related oversight of the Revolving Loan Fund program. He noted that since FY 2000, OIG has audited 50 individual revolving loan funds that identified a series of common problems. OIG issued a capping report last year on EDA's overall management of the program. The report looked at what actions EDA had taken to address the problems raised in the audit reports over the years and found that EDA had not made sufficient progress in strengthening management of the revolving loan fund program:

EDA did not have a useful central database containing current, accurate information on revolving loan fund balances or an adequate tracking and oversight system.

Grant recipients had too much cash on hand; they were not meeting EDA requirements for keeping the bulk of funds out in loans.

Recipients were not filing financial reports within required time frames and EDA was not effectively using single audit reports to manage fund assets. (Single audit reports are required by law for revolving loan funds with annual federal expenditures of \$500,000

or more.)

Mr. Zinser detailed the report's recommendations, primarily that EDA develop a comprehensive strategy and action plan that has specific measurable goals and milestones built on strong oversight from the top down. The inspector general stated that EDA responded with a 30-point action plan and has made good progress in meeting its milestones.

He stressed, however, that the most significant outstanding action item was development of a central automated database that provides current, reliable information on the entire revolving loan portfolio. At the time of his testimony, the database was slated for implementation by the spring of 2009.

Finally, Mr. Zinser noted that OIG's criminal investigations and audits of public works grants underscore the need for closer EDA scrutiny. Though OIG's oversight of these activities has been less extensive, public works audits have questioned significant costs and identified millions in funds to be put to better use. OIG investigations have uncovered instances in which grantees diverted funds to enrich themselves and as a result received prison terms and were ordered to pay fines and restitution. (*View the complete testimony at www.oig.doc.gov.*)

Assistant Inspector General for Audit and Evaluation Participates in Congressional Cyber Security Forum

On September 29, Judy Gordon, assistant inspector general for audit and evaluation, joined leaders and IT security authorities from government, business, and education for the first of three forums on cyber security, hosted by the Senate Homeland Security and Governmental Affairs Committee and the nonprofit Institute for Information Infrastructure Protection.

Challenges to securing computer systems and information grow more complex as our options for accessing them—via cell phones, MP3 players, and a host of other portable wireless technologies—multiply. The purpose of the forums is to foster greater IT security

research and development that will help public and private organization keep pace with evolving IT security challenges, and ensure critical networks and the data they carry are safeguarded.

Participants at the first forum explored IT security from the user's perspective: what environments, tools, and motivations promote safe and secure online behavior among an organization's employees and the general public? Discussions addressed, among other things, psychological and cognitive factors that prevent users from accurately assessing risk, the role of organizational culture in preventing misuse of information technology, and state and local law enforcement needs for combating electronic crime.

The remaining sessions will bring together other groups of experts to address effective IT security technologies and the economic trade-offs organizations make to secure their systems. At the conclusion of the sessions, the institute will deliver a report to the Senate subcommittee that details key findings and provides a possible roadmap for anticipating and promptly mitigating emerging security challenges.

The Institute for Information Infrastructure Protection is a national consortium of universities, laboratories, and nonprofit organizations dedicated to strengthening the U.S. cyber infrastructure.

TABLES AND STATISTICS

Statistical Overview

| TABLES | PAGE |
|--|------|
| 1. Investigative Statistical Highlights for this Period | 47 |
| 2. Audit Resolution Follow-Up | 48 |
| 3. Audit and Inspection Statistical Highlights for this Period | 48 |
| 4. Audits with Questioned Costs | 48 |
| 5. Audits with Recommendations that Funds Be Put to Better Use | 49 |
| APPENDIXES | |
| A. Report Types this Period | 50 |
| A-1. Performance Audits | 50 |
| A-2. Inspections and Evaluations | 51 |
| B. Processed Audit Reports | 52 |
| B-1. Processed Reports with Audit Findings | 52 |

Table 1. Investigative Statistical Highlights for this Period

| Criminal Investigative Activities | |
|---|--------------|
| Arrests | 3 |
| Indictments and informations | 6 |
| Convictions | 8 |
| Personnel actions | 1 |
| Fines, restitutions, judgments, and other civil and administrative recoveries | \$94,408,255 |
| Allegations Processed | |
| Accepted for investigation | 52 |
| Referred to operating units | 33 |
| Evaluated but not accepted for investigation or referral | 45 |
| Total | 130 |

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, 2008) for which no management decision had been made by the end of the period (September 30, 2008). Six audit reports remain unresolved for this reporting period (see page 53).

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, 2008) | 0 | 6 |
| Submissions | 1 | 3 |
| Decisions | 0 | 6 |
| Actions pending (September 30, 2008) | 1 | 3 |

Table 3. Audit and Inspection Statistical Highlights for this Period

| | |
|--|--------------|
| Questioned Costs | \$3,243,336* |
| Value of audit recommendations that funds be put to better use | 203,292 |
| Value of audit recommendations agreed to by management | 804,369 |

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

Table 4. Audits with Questioned Costs

| Report Category | Number | Questioned Costs | Unsupported Costs |
|---|--------|------------------|-------------------|
| Reports for which no management decision had been made by the beginning of the reporting period | 21 | \$23,629,793 | \$4,541,940 |
| Reports issued during the reporting period | 9 | 3,243,336 | 106,026 |
| Total reports (A+B) requiring a management decision during the period | 30 | 26,873,129 | 4,647,966 |
| Reports for which a management decision was made during the reporting period ² | 15 | 3,845,197 | 624,028 |
| i. Value of disallowed costs | — | 753,605 | 181,935 |
| ii. Value of costs not disallowed | — | 3,091,592 | 442,093 |
| Reports for which no management decision had been made by the end of the reporting period | 15 | 23,027,932 | 4,023,938 |

NOTES:

¹ One audit report included in this table is also included among reports with recommendations that funds be put 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

| | | Number | Value |
|--|---|--------|-----------|
| | Reports for which no management decision had been made by the beginning of the reporting period | 1 | \$104,711 |
| | Reports issued during the reporting period | 3 | 203,292 |
| Total reports (A+B) requiring a management decision during the period ¹ | | 4 | 308,003 |
| | Reports for which a management decision was made during the reporting period ² | 2 | 155,475 |
| | i. Value of recommendations agreed to by management | — | 50,764 |
| | ii. Value of recommendations not agreed to by management | — | 104,711 |
| | Reports for which no management decision had been made by the end of the reporting period | 2 | 152,528 |

NOTES:

¹ One audit report included in this table is also included among reports with questioned costs (see table 4). 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.

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 | 1 | A-1 |
| Inspections and systems evaluations | 15 | A-2 |
| Total | 16 | |

Appendix A-1. Performance Audits

| Report Title | Report Number | Date Issued | Funds to Be Put to Better Use |
|--|---------------|-------------|-------------------------------|
| Office of the Secretary | | | |
| Review of Fiscal Year 2006 Congressional Ear-marks | DEN-19021 | 05/30/08 | — |

Appendix A-2. Inspections and Evaluations

| | | | |
|---|-----------|----------|---|
| | | | |
| FY 2008 FISMA Assessment of BEA Estimation Information Technology System (BEA-015) | OSE-19001 | 09/22/08 | — |
| | | | |
| OIG Reviews Through the Decade Identify Significant Problems in Key Operations | OIG-19217 | 06/25/08 | — |
| Census Should Further Refine Its Cost Estimate for Fingerprinting Temporary Staff | OIG-10958 | 08/08/08 | — |
| FY 2008 FISMA Assessment of Wireless Data Communications General Support System (CEN28) | OSE-19163 | 09/29/08 | |
| FY 2008 FISMA Assessment of the Field Data Collection Automation System (CEN22) | OSE-19164 | 09/29/08 | — |
| | | | |
| The National Data Buoy Center Should Improve Data Availability and Contracting Practices | IPE-18585 | 05/09/08 | — |
| NOAA's Management of the Joint Enforcement Agreement Program Needs to Be Strengthened | IPE-19050 | 09/30/08 | — |
| FY 2008 FISMA Assessment of NWS Telecommunication Gateway (NOAA8871) | OSE-19000 | 09/22/08 | — |
| FY 2008 FISMA Assessment of Science and Technology System (NOAA4020) | OSE-19165 | 09/30/08 | — |
| FY 2008 FISMA Assessment of National Weather Service International Satellite Communications System (NOAA8209) | OSE-19166 | 09/30/08 | — |
| FY 2008 FISMA Assessment of Satellite Environmental Processing System (NOAA5035) | OSE-19167 | 09/30/08 | — |
| | | | |
| The Overseas Intellectual Property Rights Attaché Program Is Generally Working Well, but a Comprehensive Operating Plan Is Needed | IPE-19044 | 07/17/08 | — |
| FY 2008 FISMA Assessment of Landon IP Information System (PTOC-019-00) | OSE-19367 | 09/30/08 | — |
| FY 2008 FISMA Assessment of Enterprise Remote Access System (PTOI-011-00) | OSE-19368 | 09/30/08 | — |
| | | | |
| The Department's Privacy Impact Assessment Process Is Generally Implemented Well, But Some Improvements Are Needed | OSE-19047 | 09/24/08 | — |

Appendix B. Processed Audit Reports

The Office of Inspector General reviewed and accepted 193 audit reports prepared by independent public accountants and local, state, and other federal auditors. The reports processed with questioned costs, recommendations that funds be put to better use, and/or nonfinancial recommendations are listed in

Appendix B-1.

| Agency | Audits |
|--|------------|
| Economic Development Administration | 56 |
| International Trade Administration | 2 |
| National Institute of Standards and Technology* | 50 |
| National Oceanic and Atmospheric Administration | 29 |
| National Telecommunications and Information Administration | 2 |
| Multiagency | 54 |
| Total | 193 |

*Includes 46 ATP program-specific audits.

Appendix B-1 - Processed Reports with Audit Findings

| Report Title | Report Number | Date Issued | Funds to Be Put to Better Use | Federal Amount Questioned | Federal Amount Unsupported |
|---|------------------|-------------|-------------------------------|---------------------------|----------------------------|
| Economic Development Administration | | | | | |
| City of Baltimore Development Corporation, MD | ATL-09999-8-3244 | 09/26/08 | \$— | \$ 37,000 | \$— |
| City of Union City, CA | ATL-09999-8-3196 | 09/26/08 | — | 2,172,201 | — |
| State of Connecticut | ATL-09999-8-3171 | 09/26/08 | — | 85,468 | — |
| Southeast Idaho Council of Governments, Inc., ID | ATL-09999-8-3080 | 09/30/08 | 50,764 | — | — |
| National Institute of Standards and Technology | | | | | |
| Intrexon Corporation, VA | ATL-09999-8-3136 | 09/09/08 | — | 26,681 | 26,681 |
| Intrexon Corporation, VA | ATL-09999-8-3135 | 09/09/08 | — | 12,992 | 12,992 |
| Umbanet, Inc., NY | ATL-09999-8-3127 | 09/09/08 | 24,667 | | — |
| ISCA Technologies, Inc., CA | ATL-09999-8-3011 | 09/26/08 | 127,861 | | — |
| GE Energy (USA) LLC, DE | ATL-09999-8-3191 | 09/30/08 | — | 663,832 | — |
| Innovative Photonic Solutions, NJ | ATL-09999-8-3265 | 09/30/08 | — | 145,670 | — |

| Report Title | Report Number | Date Issued | Funds to Be Put to Better Use | Federal Amount Questioned | Federal Amount Unsupported |
|--|------------------|-------------|-------------------------------|---------------------------|----------------------------|
| National Oceanic and Atmospheric Administration | | | | | |
| Government of Guam | ATL-09999-8-3290 | 09/26/08 | — | 33,139 | — |
| State of Washington | ATL-09999-8-3174 | 09/26/08 | — | | — |
| Alaska Eskimo Whaling Commission | ATL-09999-8-3238 | 09/30/08 | — | 66,353 | 66,353 |

AUDITS UNRESOLVED FOR MORE THAN 6 MONTHS

Census Bureau

ITS Services, Inc. In March 2005, we reported that 3 of the 32 task orders awarded under an 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 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 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.

NIST

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 led to a criminal investigation, which resulted in a conviction (see page 41). Audit resolution is suspended, pending sentencing in October 2008.

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 | | Page |
|---------------------|---|-------|
| 4(a)(2) | Review of Legislation and Regulations | 54-55 |
| 5(a)(1) | Significant Problems, Abuses, and Deficiencies | 13-43 |
| 5(a)(2) | Significant Recommendations for Corrective Action | 13-43 |
| 5(a)(3) | Prior Significant Recommendations Unimplemented | 54 |
| 5(a)4 | Matters Referred to Prosecutive Authorities | 47 |
| 5(a)(5) and 6(b)(2) | Information or Assistance Refused | 55 |
| 5(a)(6) | Listing of Audit Reports | 50-53 |
| 5(a)(7) | Summary of Significant Reports | 13-39 |
| 5(a)(8) | Audit Reports—Questioned Costs | 48 |
| 5(a)(9) | Audit Reports—Funds to Be Put to Better Use | 49 |
| 5(a)(10) | Prior Audit Reports Unresolved | 55 |
| 5(a)(11) | Significant Revised Management Decisions | 55 |
| 5(a)(12) | Significant Management Decisions with Which OIG Disagreed | 55 |

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 reports and one NIST report 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 six 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.