U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

TOP TEN MANAGEMENT CHALLENGES
September 2004

MAJOR CHALLENGES
FOR THE
U.S. DEPARTMENT OF COMMERCE

TOP 10 CHALLENGES

1. Strengthen Department-wide information security.
2. Effectively manage departmental and bureau acquisition processes.
3. Successfully operate USPTO as a performance-based organization.
4. Control the cost and improve the accuracy of Census 2010.
5. Increase the effectiveness of marine resource management.
6. Promote fair competition in international trade.
7. Enhance export controls for dual-use commodities.
8. Enhance emergency preparedness, safety, and security of Commerce facilities and personnel.
9. Continue to strengthen financial management controls and systems.
10. Continue to improve the Department's strategic planning and performance measurement in accordance with GPRA.

The Office of Inspector General, in assessing its work at the close of each semiannual period, develops its list of Top 10 Management Challenges the Department faces. Each challenge meets one or more of the following criteria: (1) it is important to the Department's mission or the nation's well-being, (2) it is complex, (3) it involves sizable resources or expenditures, or (4) it requires significant management improvements. Because of the diverse nature of Commerce activities, these criteria sometimes cut across bureau and program lines. Experience has shown that by aggressively addressing these challenges the Department can enhance program efficiency and effectiveness; eliminate serious operational problems; decrease fraud, waste, and abuse; and achieve substantial savings.

CHALLENGE 1

STRENGTHEN DEPARTMENT-WIDE INFORMATION SECURITY

Many of Commerce's information technology systems and the data they contain have national significance. Loss of or serious damage to any of these critical systems could have devastating impacts. Therefore, identifying weaknesses in them and recommending solutions is a continuing top priority for the Office of Inspector General. The Federal Information Security Management Act of 2002 (FISMA) provides a comprehensive framework for ensuring that information resources supporting federal operations and assets employ effective security controls. FISMA requires OIGs to perform independent security evaluations of their agencies annually.

Examples of Critical Data Processed by Commerce IT Systems

- The Bureau of Industry and Security's export license data helps control the release of dual-use commodities to countries and entities of concern.
- The National Oceanic and Atmospheric Administration's satellite, radar, and weather forecasting data and systems provide information used to protect lives and property.
- The Economics and Statistics Administration's economic indicators have policymaking implications that can affect the movement of global commodity and financial markets.
- The U.S. Patent and Trademark Office's patent and trademark information is essential to administering patent and trademark law, promoting industrial and technical progress, and strengthening the national economy.

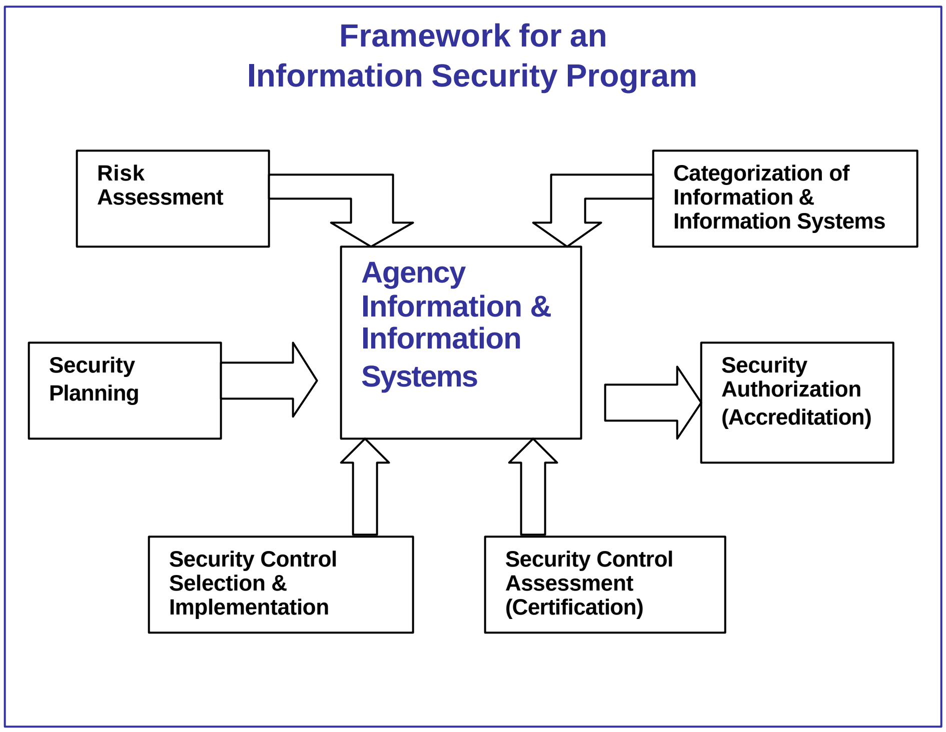
During this fiscal year the Department has continued to focus on improving information security. On June 29, 2004, the Secretary issued a memorandum highlighting the need for giving high priority to information security: he directed secretarial officers and heads of operating units to allocate sufficient resources for this purpose, support their unit's chief information officer (CIO) in managing information security, and ensure that senior program officials who authorize systems to operate have received sufficient training in the certification and accreditation (C&A) process. When implemented properly, certification is a powerful tool for helping ensure that appropriate security controls are in place, functioning as intended, and producing the desired outcome. Through accreditation, agency officials formally accept responsibility for the security of the systems over which they have management, operational, and budget authority and for any adverse impacts to the Department if a breach of security occurs.

The Department's CIO has continued to push completion of system certifications and accreditations; updated Commerce's information security policy on such topics as managing the IT system inventory, assessing security controls, and preparing plans of action and milestones for remediating security weaknesses; and developed a policy on peer-to-peer file sharing.[1] But similar to last year's FISMA review, our FY 2004 evaluation found that the Department still faces considerable challenges in adequately safeguarding the hundreds of Commerce systems, particularly with regard to effectively conducting these critical activities: (1) assessing risk and determining appropriate security controls, (2) testing and evaluating these controls, (3) certifying and accrediting systems, and (4) ensuring that personnel with specialized information security

[1] Peer-to-peer file sharing allows individual users of the Internet to connect directly through the Internet to each other so as to transfer or exchange computer files.

responsibilities receive the necessary training. (See September 2004 *Semiannual Report*, page 42.)

The Census Bureau is a case in point. Our review of the bureau's information security program found significant deficiencies in its C&A documentation and processes, such as risk assessments that did not sufficiently identify system vulnerabilities, and security plans that assigned improper and inconsistent sensitivity levels to systems and did not adequately describe the controls that were in place or needed (see September 2004 issue, page 23). The documentation also did not identify residual risks in the certified and accredited systems, and thus provided no evidence that the accrediting official understood the level of risk being assumed in authorizing system operations.



Source: http://csrc.nist.gov/organizations/fissea/conference/2004/presentations.html, accessed October 5, 2003.

For the past 3 fiscal years, the Department reported information security as a Federal Management Financial Integrity Act (FMFIA) material weakness in its *Performance & Accountability Report*, in part because our reviews of the C&A documentation for numerous national- and mission-critical systems reported as certified and accredited have continued to identify significant deficiencies.

This year we again reviewed the C&A documentation for a sample of the Department's national-critical and mission-critical systems reported as certified and accredited. Although we observed some improvements, our review found serious shortcomings in the risk assessments, security plans, contingency plans, and testing to ensure that security controls are implemented and working as intended. Thus, we recommended that information security should remain a material weakness for FY 2004. Nevertheless, we were pleased to note some progress. In particular, based on our review of C&A documentation, we found the C&A processes of the Bureau of Economic Analysis and Office of the Secretary provide reasonable assurance that their national- and mission-critical systems are adequately protected.

MATERIAL WEAKNESS AT USPTO RESOLVED

Like the Department, USPTO reported information security as a material weakness in prior-year *Performance & Accountability Reports*, which it submits separately. However, USPTO has reported all of its critical systems as certified and accredited, and we are pleased to report that our review of a sample of C&A materials confirmed the adequacy of its C&A process and documentation. We therefore consider USPTO's material weakness resolved.

DEPARTMENT-WIDE CONTRACT SECURITY DEFICIENCIES REMAIN

We noted in our FY 2003 FISMA report that inadequate security provisions in Commerce IT service contracts also place systems at risk. The Department continued to rely heavily on contractors to provide IT services, spending 65 percent of its IT contract dollars in this area in FY 2003. Last year's FISMA evaluation found that while progress had been made in incorporating security provisions into recent IT service contracts, provisions for controlling contractor access to Department systems and networks were generally absent, and there was little evidence of contract oversight or of coordination among contracting, technical, and information security personnel in developing appropriate contract security. This year we provided additional analysis of the contract security issues as well as recommendations to further ensure that information and information systems are adequately secure when contractor-provided services are used. Specifically, we recommended that Commerce take steps to ensure that its service contracts contain the new security clauses, issued in November 2003, and that appropriate contract oversight occurs. (See September 2004 *Semiannual Report*, page 43.)

COMPUTER INCIDENT RESPONSE WEAKNESSES NOTED

As part of our FISMA work, we evaluated Commerce's computer incident response capability and found that its decentralized structure is appropriate for the Department's diverse and multiunit organization. (See September 2004 *Semiannual Report*, page 43.)However, we identified numerous weaknesses:

- No centralized entity to promote information sharing and consistency in response processes.
- Inadequate incident response procedures.
- Incomplete and inconsistent incident reporting by the operating units.
- The need for better intrusion detection approaches and specialized tools and training.

The Department CIO concurred with our findings and is taking action to improve Department-wide incident detection and response.

CHALLENGE 2

EFFECTIVELY MANAGE DEPARTMENTAL AND BUREAU ACQUISITION PROCESSES

Federal acquisition legislation in the 1990s mandated sweeping changes in the way federal agencies buy goods and services. The intent was to reduce the time and money spent on purchasing and improve the efficiency of the process. The latest legislative effort to streamline acquisition is the Services Acquisition Reform Act of 2003, whose provisions further push for performance-based service contracting: the act provides that service contracts under $25,000 may be treated as "commercial" if certain performance-based criteria are met and thereby be eligible for simplified acquisition procedures. As the Department's reliance on contractor-provided services increases, so does the challenge to effectively manage the streamlined acquisition processes these initiatives fostered, while ensuring that taxpayer dollars are wisely spent and laws and regulations followed.

This balance is best maintained by adhering to basic acquisition principles: careful planning, promotion of competition, prudent review of competitive bids, adept contract negotiations, well-structured contracts, and effective contract management and oversight. These are essential to ensuring that sound contracting decisions are made and contracts successfully executed. Problems we have identified with service contracting in the past include failure to use performance-based task orders where they would be beneficial, inadequate training in the use of performance-based service contracting, insufficient planning for contract administration and monitoring, and failure to ensure that adequate security provisions are included and enforced in IT service contracts.

The Department has recently taken a number of steps to improve management of Commerce acquisition processes. In March 2004, it mandated the use of standardized clauses for IT security for all applicable solicitations and contracts, and as part of the Department's annual IT security compliance review, its Office of Acquisition Management (OAM) worked with the CIO's office to determine whether such clauses are being included in IT service contracts. Additionally, OAM has established a board to review the Department's major acquisitions, competitive sourcing opportunities, and interagency agreements; and it reports having achieved the goal of using performance-based acquisitions to award not less than one-half of the total dollar amount the Department expends on service contracts.

OIG ACQUISITION REVIEWS CONTINUE

The serious consequences of poor contract management were evident in our review last year of a NOAA/NWS contract modification for a transition power source for the NEXRAD weather radar, which resulted in NWS paying for defective equipment, contract costs increasing by an estimated $4.5 million, and the purchase of a product that may not have been the best choice for NEXRAD. (See September 2003 *Semiannual Report*, page 25.) OIG continues to monitor the corrective action plan being implemented as a result of this review and is working with NOAA's director of acquisitions and grants to improve the consistency and thoroughness of NOAA's acquisition process. NWS has also taken actions in response to OIG's recommendations, including issuing a policy directive on acquisition management, and indicates that a critical element on procurement has been added to the performance plans of staff involved in the acquisition process.

Currently, we are reviewing NIST's contract administration process. Our objectives are to determine whether NIST has (1) effective policies and procedures for processing and managing procurement actions in accordance with pertinent laws and regulations, (2) an acquisition workforce that is adequately trained and skilled to handle NIST's procurement actions, and (3) a system for effectively and efficiently processing procurements in accordance with Commerce/NIST policies and procedures.

MAJOR CONSTRUCTION AND RENOVATION PROJECTS

Contracts for large, costly, and complex capital improvement and construction projects carry numerous inherent risks. This is an area of particular vulnerability for the Department, given the many construction and/or renovation projects it has planned or under way for Commerce facilities. For this reason, we continue to monitor the progress of some of the Department's key current and planned construction projects.

Artist's rendering of planned NOAA Fisheries research facility in Juneau.
Source: http://www.fakr.noaa.gov/lena/renderings.htm, accessed October 15, 2004.

We have just concluded a review of USPTO's progress in completing, furnishing, and occupying its new headquarters complex in northern Virginia (see Challenge 3 and page 39 of the September 2004 issue). We also plan to keep abreast of other major Commerce renovation and construction projects, such as Census's construction of its new Suitland, Maryland, headquarters; the Department's planned renovation of its headquarters (the Herbert C. Hoover Building in Washington, D.C.); and NOAA's construction of a Pacific Region Center in Hawaii and a fisheries research facility in Juneau, Alaska.

CHALLENGE 3

SUCCESSFULLY OPERATE THE U.S. PATENT AND TRADEMARK OFFICE AS A PERFORMANCE-BASED ORGANIZATION

The United States Patent and Trademark Office's operation as a performance-based organization continues to warrant special attention. USPTO maintains that the efficiency with which it issues patents has a huge impact on the pace of technological advancement worldwide. The prompt registration of trademarks protects commercial investment, informs consumer choices, and promotes the availability of new goods and services.

USPTO has assumed responsibility for certain operational functions that were once controlled or monitored at the departmental level, and it is essential that the bureau effectively use its expanded authority over budget allocations and expenditures, personnel decisions and processes, procurement, and information technology operations to support the issuance of patents and trademarks.

Since 2002, USPTO has been working to implement its *21st Century Strategic Plan*. The 5-year plan was intended to help the agency overcome the challenges accompanying its transition to performance-based operations, successfully develop necessary personnel policies, establish procurement and administrative policies as well as performance-oriented processes and standards for evaluating cost-effectiveness, and meet its performance goals under the Government Performance and Results Act (GPRA).

Key USPTO Patent Statistics 2003

Patent Examiners	**3,579**
Applications Filed	**333,452**
Applications Granted	**173,072**
Backlog	**457,254**
First Actions	**283,111**
Final Disposals	**284,470**
Average Pendency	**26.7mos.**

Source: USPTO

According to the agency, the plan provides a roadmap for major changes in patent and trademark processes. These include steps to (1) improve and maintain patent and trademark quality, (2) move to a paperless environment and promote e-government, (3) enhance employee development, and (4) explore competitive sourcing. The plan also calls for the agency to work with international intellectual property offices to create a global framework for enforcing intellectual property rights.

Our office recently performed three reviews at USPTO. First, we reviewed patent examiner production goals, performance appraisal plans, and awards to determine their effect on the output of the patent examiner corps. We found that patent examiner goals have not changed since 1976 to reflect efficiencies in work processes; patent examiners' performance appraisal plans are not linked to their supervisors' goals or those of USPTO; and patent examiner awards do not appear to be having their intended impact of stimulating examiner production. (See September 2004 *Semiannual Report*, page 38.)

Second, we reviewed progress on construction of the agency's new, state-of-the-art headquarters complex in Alexandria, Virginia, and its relocation to these facilities. This project is one of the federal government's largest real estate ventures. When completed in 2005, the 5-building complex will bring together the majority of USPTO employees and contractors, who are currently scattered among 18 buildings in Crystal City, Virginia. USPTO has already occupied 3 of the new buildings and expects to take occupancy of the remaining 2 earlier than anticipated. We found, among other things, that USPTO and GSA have provided adequate management and financial oversight of the project; USPTO successfully planned and executed its recent move of 2,093 employees to the 2 buildings completed at the time of our review; and cost increases that have occurred are due primarily to project delays beyond USPTO's control, as well as to new requirements, such as information technology changes and security upgrades. (See September 2004 issue, page 39.)

Artist's rendering of USPTO's five-building complex in Alexandria, Virginia, clockwise from lower left: Remsen, Jefferson, Madison, Knox, and Randolph.
***Source*:** USPTO

Third, in response to complaints and a request from the agency's chief financial officer/chief administrative officer, we reviewed certain aspects of the Office of Human Resources (OHR). We found among other things that the recruitment process for the human resources director position was flawed and that USPTO, in collaboration with the Department, needed to clarify its relationship with the Office of Personnel Management and establish sufficient human resources policies and procedures. (See September 2004 *Semiannual Report*, page 40.)

CHALLENGE 4

CONTROL THE COST AND IMPROVE THE ACCURACY OF CENSUS 2010

Few Commerce activities have more ambitious goals, higher costs, or more intensive resource requirements than the constitutionally mandated decennial census, and with each decade, this undertaking becomes more costly, complex, and challenging. Costs of $2.2 billion in 1980 rose to $3.3 billion in 1990 and to $6.6 billion in 2000. They have been estimated to be $9.3 billion in 2010 (in constant 2000 dollars).

Achieving an accurate population count has become more difficult and costly over the past 3 decades because the nation's population has increased and diversified dramatically. And much has changed in the methods and technologies used for decennial census taking during that time. But the primary weaknesses we noted in monitoring the 1980, 1990, and 2000 decennials have remained the same and are at least partially responsible for the ballooning costs: insufficient planning and lack of upfront funding for an undertaking that by its very nature requires long-term vision and development, as well as appropriate testing at key points along the way.

PLANNED DECENNIAL CENSUS TESTS

Site Tests	2004 Census Test 2006 Census Test
National Tests	2003 National Census Test 2005 National Census Test
Overseas Tests	2004 Overseas Census Test 2006 Overseas Census Test
Dress Rehearsal	2008

Source: U.S. Census Bureau

The Census Bureau has taken numerous steps toward improving 2010 operations and controlling costs. In September 2002 it adopted a reengineered framework for conducting the decennial: an American Community Survey to collect and tabulate long-form data throughout the decade; an enhanced address list and geographic information database; and a program of early planning, development, and testing for a short-form-only census. The three-pronged strategy is ambitious and intended to capitalize on the latest technology, such as handheld computers equipped with global positioning system capabilities for field operations, including address canvassing and nonresponse follow-up data collection.


The palm-sized handheld computer used for the 2004 NRFU operation.

In this semiannual period, we assessed the 2004 census test (see September 2004 *Semiannual Report*, page 20), in which the bureau tested, among other things, the feasibility of using handheld computers to automate nonresponse follow-up (NRFU). The test was conducted in a portion of New York City and in three rural counties in south central Georgia. We found that the handheld computers and related automation are promising replacements for paper-based processes, and the enumerator workforce was able to use the handhelds.

However, the test exposed issues that will have to be addressed for future tests and the 2010 census, including problems with data transmissions, technical support to the field, and the bureau's system and software engineering practices. Among other areas we noted in need of improvement were enumerator training, planning for tests of revised group quarters definitions, and several management and administrative activities.

We will continue our focus on the bureau's planning for the 2010 decennial, including its preparation for the 2006 site test, as well as review other issues and related matters that could have an impact on the decennial.

CHALLENGE 5

INCREASE THE EFFECTIVENESS OF MARINE RESOURCE MANAGEMENT

The National Marine Fisheries Service (NOAA Fisheries) must balance two competing interests: (1) promoting commercial and recreational fishing as vital elements of our national economy and (2) preserving populations of fish and other marine life. The Magnuson-Stevens Act of 1976, the Marine Mammal Protection Act of 1972, and the Endangered Species Act of 1973 gave NOAA Fisheries responsibility for rebuilding and maintaining sustainable fisheries and promoting the recovery of protected marine species. The Magnuson-Stevens Act also made NOAA Fisheries the primary federal agency for managing marine fisheries and established a regional fishery management system to help the agency carry out its mission. The 1996 amendments to the act strengthened NOAA Fisheries' role in protecting and sustaining fisheries and their habitats.

PACIFIC COASTAL SALMON RECOVERY FUND

Established by Congress in 2000 at the request of the states of Washington, Oregon, California, and Alaska, the Pacific Coastal Salmon Recovery Fund provides grants to these states and their resident Native American tribes to support local salmon conservation efforts. The fund is the third largest source of federal support for salmon recovery efforts and the largest financial assistance program in this area administered by NOAA.

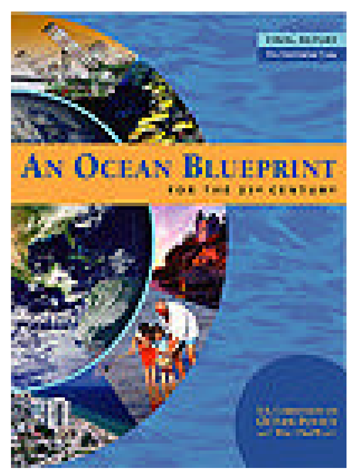
Given the millions of dollars at stake and the importance of the NOAA program, we turned our attention this semiannual period to salmon recovery fund awards, concluding the first three in a series of planned audits.

Pacific Coastal Salmon Recovery Funding Administered by NOAA (in millions)						
	FY 2000	**FY 2001**	**FY 2002**	**FY 2003**	**FY 2004**	**Totals**
Washington	$18.0	$30.2	$34.0	$27.8	$26.0	$136.0
Alaska	$14.0	$19.5	$27.0	$21.9	$20.6	$103.0
California	$9.0	$15.1	$17.0	$13.9	$13.0	$68.0
Oregon	$9.0	$15.1	$17.0	$13.9	$13.0	$68.0
Idaho	$.00	$.00	$.00	$.00	$4.9	$4.9
Pacific Coastal Tribes	$6.0	$7.4	$11.0	$8.9	$8.4	$41.7
Columbia River Tribes	$2.0	$2.5	$4.0	$3.0	$3.1	$14.6
Total	$58.0	$89.8	$110.0	$89.4	$89.0	$436.2

Source: FY 2000-2004 figures at http://webapps.nwfsc.noaa.gov/servlet/page?_pageid=1292&_dad=portal30&_schema=PORTAL30, accessed October 15, 2004; totals provided by OIG.

Our initial reviews focused on programs operated by an Oregon state agency and a Washington state Indian commission. In each case, we questioned significant portions of costs claimed by the recipients and recommended recovery of federal funds. We are keeping NOAA advised of the results of our ongoing audits so that the agency is able to address common issues through strengthened grants management.

U.S. COMMISSION ON OCEAN POLICY



In September 2004, the U.S. Commission on Ocean Policy presented its final report—*An Ocean Blueprint for the 21st Century*—detailing its findings regarding the state of our nation's ocean and coastal resources, and offering recommendations for building a coordinated and comprehensive national ocean policy. The last comprehensive review of U.S. ocean policy was conducted 35 years ago. Since then, our oceans and coasts have changed drastically—more than 37 million people, 19 million homes, and countless businesses have been added to coastal areas.

In its report, the commission called for, among other things, a review of all federal agencies with ocean-related responsibilities, with an eye toward eliminating redundant programs, and recommended greatly expanding NOAA's environmental stewardship activities. The areas identified in the commission's report, especially those concerning NOAA's broader environmental stewardship responsibilities, will draw our attention in the future.

CHALLENGE 6

PROMOTE FAIR COMPETITION IN INTERNATIONAL TRADE

To compete effectively in today's global marketplace, many U.S. companies need help accessing new or expanded export market opportunities as well as addressing unfair trade practices, trade disputes with foreign firms, noncompliance with or violations of trade agreements, inadequate intellectual property protection, and other impediments to fair trade. Commerce must ensure that its export promotion assistance and trade compliance and market access efforts adequately serve U.S. exporters, and its enforcement of U.S. trade laws helps eliminate unfair competition from imports priced at less than fair market value or subsidized by foreign governments.

To help meet the challenges in highly competitive world markets, Commerce and its International Trade Administration (ITA) work with the Office of the U.S. Trade Representative, the Departments of State and Agriculture, and numerous other federal agencies to monitor and enforce trade agreements. The number and complexity of those agreements have increased substantially in recent years, and the Secretary of Commerce has made monitoring and enforcing trade agreements and laws a top priority for ITA and the Department as a whole. Over the years, Commerce has received additional funding for trade compliance activities, such as placing compliance officers overseas in several key markets. Increased funding has enabled ITA to attract needed staff without having to request special hiring authority or offer recruitment incentives (see March 2003 *Semiannual Report*, page 20).

> Commerce has numerous mechanisms to monitor and help enforce U.S. trade agreements and review trade complaints. When warranted, its Trade Compliance Center forms teams to follow up on complaints and bring them to satisfactory conclusion. ITA's overseas offices, operated by the U.S. and Foreign Commercial Service, and its other operating units perform a substantial amount of market access and trade compliance work. Overall, ITA's approach to trade compliance and market access is to engage the issue at the working level wherever possible, thus avoiding formal dispute settlement structures such as the World Trade Organization, which can take years to resolve trade disagreements. The Department and ITA pursue important matters of policy—such as intellectual property rights protection, standards development, trading rights, and distribution services—in government-to-government negotiations.

Commerce's many overseas posts and domestic U.S. export assistance centers (USEACs) help U.S. companies identify specific export marketing opportunities and trade leads and offer other trade promotion and export finance counseling services, especially to small and medium-size firms that are new to exporting or seeking to expand their overseas markets. During this past year, we reviewed three USEAC networks—Chicago, Pacific Northwest, and Philadelphia—that comprise 28 individual centers operated by ITA's Commercial Service. We evaluated their management operations and ability to provide value-added export counseling to U.S. companies (see March 2004 *Semiannual Report*, page 24). During this semiannual period, we released a crosscutting report on strengths and weaknesses common to the networks (see September 2004 issue, page 25). In each network, we found that client satisfaction was high, strong relationships existed with local partners, and financial and administrative operations were generally sound. However, we also noted inconsistencies in reporting and oversight that led to overstated export success dollar values—a key barometer of performance. Since we first identified problems with export success reporting, ITA and Commercial Service have taken a number of steps to improve related quality controls and oversight of the process, and they are working to train managers and staff in correct reporting procedures. However, further improvements are needed in the reporting guidelines and management accountability.

Our USEAC findings mirrored those of our recent reviews of overseas operations. Inspections of Commercial Service posts in Greece and Turkey revealed that, again, most customers were satisfied with the products and services they received, but both posts had overstated the value of their export successes. (For more detail on Greece, see September 2003 *Semiannual Report*, page 22. For Turkey, see the March 2003 issue, page 19.)

We also report in this issue the findings of our inspection of Commercial Service's post in India (see September 2004 *Semiannual Report*, page 26). We found that the post is generally doing a good job of providing export assistance to U.S. companies and collaborates well with its trade partners, other components of the U.S. mission and ITA, and other government agencies. But as at the USEACs and other overseas posts we have inspected, the India post's reported export successes were problematic. In many cases we could not verify the link between Commercial Service assistance and the reported export success, and we identified several that did not meet the criteria of an export success. Although, as noted earlier, Commercial Service and ITA have taken steps to improve management oversight of reporting, we are concerned that Commercial Service's new, written FY 2004 reporting guidelines have reduced management accountability for ensuring the accuracy and integrity of export success reports. We will continue to monitor these areas and report on the Department's efforts to resolve issues we identify.

CHALLENGE 7

ENHANCE EXPORT CONTROLS FOR DUAL-USE COMMODITIES

The National Defense Authorization Act (NDAA) for Fiscal Year 2000, as amended, directed the inspectors general of the Departments of Commerce, Defense, Energy, and State, in consultation with the directors of the Central Intelligence Agency and the Federal Bureau of Investigation, to report to Congress by March 30, 2000, and annually until the year 2007, on the adequacy of export controls and counterintelligence measures to prevent the acquisition of sensitive U.S. technology and technical information by countries and entities of concern. In addition, NDAA for FY 2001 requires the IGs to discuss in their annual interagency report the status or disposition of recommendations made in earlier reports submitted in accordance with the act.

Our FY 2004 NDAA work dealt with the effectiveness of dual-use deemed export regulations and policies,[2] including their implementation by BIS, and compliance with

[2] According to the Export Administration Regulations, any release to a foreign national of technology or software subject to the regulations is deemed to be an export to the home country of the foreign national.

the regulations by U.S. industry, Commerce agencies, and academic institutions. (See March 2004 *Semiannual Report*, page 14.) We found that certain aspects of BIS' deemed export outreach program are working well, but we also identified problems that hamper the efforts of both BIS and the U.S. government to more effectively prevent the transfer of sensitive technology to foreign nationals from countries or entities of concern while they are in the United States. In addition, our most recent follow-up report on prior OIG recommendations noted closure of all outstanding issues from 2000, but numerous recommendations from subsequent years are still open. (See March 2004 *Semiannual Report*, page 17.) BIS has since submitted an action plan to address our deemed export recommendations and notes that it is developing a deemed export compliance program and deciding whether to modify its regulations and public guidance. It also reports having increased its deemed export educational outreach to companies, universities, and research institutions.

For the 2004 interagency report, the IG review team (Commerce, Defense, Energy, State, and the CIA) and the Department of Homeland Security's OIG[3] completed a crosscutting review of the adequacy and effectiveness of government-wide efforts to promote compliance with deemed export control laws and regulations and to determine whether they protect against the transfer of controlled U.S. technologies and technical information. (See September 2004 *Semiannual Report*, page 14.)

REVIEW OF THE EXPORT LICENSING PROCESS FOR CHEMICAL AND BIOLOGICAL COMMODITIES

To comply with NDAA's FY 2005 requirement, we are reviewing the export licensing process for chemical and biological commodities to determine whether current licensing and enforcement practices are consistent with relevant laws and regulations, as well as established national security and foreign policy objectives, such as those set forth in the President's *National Strategy to Combat Weapons of Mass Destruction* (December 2002). In addition, we are assessing the effectiveness of coordination between the various federal agencies during the export licensing process for these commodities.

While BIS, the administration, and Congress work to target federal licensing and enforcement efforts on exports that present the greatest proliferation and national security risks, and streamline or eliminate controls that hamper trade and are not necessary to address national security or foreign policy concerns, congressional enactment of a new Export Administration Act is vital to the success of the U.S. government's efforts to enhance export controls. We will continue to monitor BIS' efforts to improve the effectiveness of dual-use export controls.

These exports are commonly referred to as "deemed exports" and may involve the transfer of sensitive technology to foreign visitors or workers at U.S. research laboratories and private companies.

[3] Homeland Security participated in the 2004 assessment because of the nature of the review topic.

CHALLENGE 8

ENHANCE EMERGENCY PREPAREDNESS, SAFETY, AND SECURITY OF COMMERCE FACILITIES AND PERSONNEL

Since our March 2002 report on the status of emergency preparedness and security programs at a cross-section of Commerce facilities, the Department has made significant improvements, but the challenge remains. Heightened security requires a variety of measures: infrastructure risk assessments, emergency backup sites, upgraded physical security, and employee awareness and training, to name a few. Despite progress in these areas, the Department needs to regularly reassess its security status to ensure it provides adequate protections for employees and operations, and must make modifications as needed.

Commerce has reported a number of actions to enhance security thus far this year. This includes drafting a new Department Administrative Order relating to foreign national visitors and guest researchers in Commerce facilities, which is currently being reviewed by Commerce bureaus. The Department also reported that it has conducted numerous risk assessments of Commerce facilities and compliance reviews of security containers[4] and classified documents to help ensure the safety of Commerce personnel and national security information. Commerce's Office of Security is also working with bureaus to develop or update their continuity of operations and emergency operations plans.

Given the size of its workforce and the geographical spread of its hundreds of facilities nationwide and at more than 150 overseas locations, complying with recent security-related guidance is a complex, resource-intensive undertaking for Commerce. Our inspections of overseas posts and domestic U.S. export assistance centers operated by the Commercial Service identified the need for more timely security upgrades, improved oversight of security operations, and in some cases, specific security improvements.

We believe Commerce is making progress on many emergency preparedness, safety, and security fronts, but the challenge is massive. OIG is currently conducting a follow-up review of the Department's emergency preparedness efforts to ascertain the status of these activities and to identify other areas that may still need to be addressed.

CHALLENGE 9

CONTINUE TO STRENGTHEN FINANCIAL MANAGEMENT CONTROLS AND SYSTEMS

Federal law requires agencies to prepare and disseminate financial information, including audit reports on their financial statements, to enable Congress, agency executives, and the

[4] Security containers are secure receptacles (e.g., safes) or holding areas for classified documents and materials.

public to assess an agency's operational and program management and to determine whether its financial management systems comply with legislative mandates.

The Department has now implemented the Commerce Administrative Management System, achieved and maintained unqualified opinions on its consolidated financial statements, and come into substantial compliance with the Federal Financial Management Improvement Act—all significant accomplishments. These successes reflect management's commitment to and success at addressing the findings of deficient internal controls and financial management systems identified in our audits and other reviews over the past decade.

Nevertheless, maintaining sound financial management controls and systems remains a challenge, given the Department's size, the diversity of its mission-related activities, its complex mix of financial systems and operations, and the billions of dollars it must account for each year. We will continue to monitor a range of financial management issues, including Commerce's progress in meeting the accelerated financial reporting dates required by OMB for the FY 2004 financial statements audit—now due just 45 days after year-end; the effectiveness of the Department's internal controls; the International Trade Administration's progress toward implementing full cost recovery to comply with OMB Circular A-25; and the Department's maintenance and operation of financial systems, including change management for updating software.

CHALLENGE 10

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

Congress and agency managers require relevant performance measures and credible performance data to effectively oversee federal programs. The Government Performance and Results Act of 1993 was designed to ensure the availability of such data by mandating that agencies set goals for program performance and report outcomes measured against them. Accurate performance results are essential to agencies' ability to develop integrated budget and performance information and to make sound funding decisions.

Over the past several years, we have reviewed the collection and reporting of performance data by eight of Commerce's largest operating units. Our audits have identified the need for (1) stronger internal controls to ensure that reported data is accurate, (2) measures that clearly articulate what is being assessed, and (3) improved explanations and disclosures to clarify and enhance the usefulness of the results.

During this past semiannual period, these same issues emerged in our audit of NOAA performance measures supporting the agency's goals of building sustainable fisheries, recovering protected species, and predicting and assessing decadal to centennial climate change. We found that reporting for all three of the goals was problematic: in some cases, titles of measures did not clearly convey what was being assessed; in others, explanations and verification details were incomplete, or supporting documentation was inadequate. To correct these deficiencies, NOAA needs to (1) revise or otherwise clarify certain performance measures, (2) strengthen internal controls to ensure that reported data is fully supported and adequately explained, and (3) provide complete and appropriate detail in discussions of results. (See September 2004 *Semiannual Report*, page 29.)

The operating units for which we have completed performance measure audits have been responsive to our recommendations: they have developed action plans to address identified deficiencies and have revised previously reported performance information accordingly. As each unit takes such steps, we are confident that performance data will become more reliable and useful, and thus better serve the purpose and intent of GPRA.