DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

Office of Audits

OIG-05-06 December 2004

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report presents OIG's assessment of "major management challenges" facing DHS. It is based on issued reports, interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents. These challenges are a major factor in setting OIG's priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, OIG updates its assessment of management challenges annually for inclusion in DHS' Performance and Accountability Report.

It is my hope that this report will result in more effective, efficient, and economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin
Inspector General

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

November 1, 2004

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

During its first 20 months of existence, the Department of Homeland Security (DHS) worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented many challenges to the department's managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization.

The Office of Inspector General (OIG) identified "major management challenges" facing the department, as discussed below. These challenges are a major factor in setting DHS OIG priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, the OIG will update its assessment of management challenges annually.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components into a single, effective, efficient, and economical department remains one of DHS' biggest challenges. DHS has made notable progress in this area. For example, DHS established an Operational Integration Staff to assist departmental leadership with the integration of certain DHS missions, operational activities, and programs at the headquarters level and throughout the DHS regional structure. However, much remains to be done and structural and resource problems continue to inhibit progress in certain support functions.

For example, while the department is trying to create integrated and streamlined support service functions, most of the critical support personnel are distributed throughout the components and are not directly accountable to the functional Line of Business (LOB) Chiefs. On the other hand, the Chief Procurement Officer (CPO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO), and Chief

of Administrative Services (CAS) have been directed to lead the development of management and integration efforts for their respective function, and have been given the responsibility of optimizing a department-wide support structure that eliminates redundant efforts.

In August 2004, the Secretary and Deputy Secretary directed the DHS LOB Chiefs to design and implement systems that will optimize their functions across the entire department and develop Management Directives to guide the department's management of that business function. The Directives are to build on a concept of "dual accountability" where both the operational leadership and the LOB chiefs are responsible for the successful preparation of Directives that will govern the work and the implementation effort that follows their preparation. The Deputy Secretary described the concept as a "robust dotted line" relationship of agency or component functional heads to the LOB chiefs for both daily work and annual evaluation. Final Management Directives are expected to provide direction for both process and resource management. The Secretary and Deputy Secretary called for these documents to be issued in mid-September 2004 in order to institutionalize the arrangements before FY 2005. As of October 15, while the department had not released any final Management Directives, the department's Management Council and appropriate departmental councils (i.e., CIO Council, etc.) had approved each of the Management Directives related to each LOB. In addition, Council charters have been signed for each LOB that signify concurrence among the organizational elements (OEs) of the department and establishes a formal governance and advisory board structure to ensure that the objectives and intent of the Directives are executed.

OIG will be monitoring and evaluating these efforts closely.

CONTRACT MANAGEMENT

DHS obligated about $6.8 billion procuring goods and services during FY 2003. In addition to the challenge of integrating the procurement functions of its component organizations, DHS must provide contract management to the OEs that came into the agency without the accompanying procurement staff. These components include the Science and Technology (S&T) Directorate, the Information Analysis and Infrastructure Protection (IAIP) Directorate, the Office of State and Local Government Coordination and Preparedness, U.S. VISIT, and other departmental operations. DHS formed the Office of Procurement Operations (OPO) to provide procurement support for these components, but the office has insufficient staff to manage over $2.5 billion in procurements. DHS has contracted with other federal agencies to provide the contract management support needed while it addresses the resource issues in OPO. However, providing consistent contract management throughout DHS remains a formidable challenge. The OPO has developed and negotiated with its customer organizations a staffing plan for OPO that would bring OPO's staffing level to 127 by the end of FY 2005. The cost of these positions would be reimbursed by customer organizations through the Working Capital Fund.

DHS' efforts to provide a sufficiently detailed and accurate listing of procurement information proved difficult and were hampered by existing federal systems. While DHS has migrated all of its procurements under the umbrella of one comprehensive reporting system, the department still lacks sufficiently detailed and validated data for FY 2003 and FY 2004 to manage the procurement universe and ensure accurate and consistent reporting.

The DHS OEs also face continuing challenges in contract management, but have made some progress. For example, the Transportation Security Administration (TSA) relies extensively on contractors to accomplish its mission, but during its first year of operation, provided little contract oversight. As a result, the cost of some of those initial contracts ballooned. In 2004, however, TSA began implementing policies and procedures to provide improved procurement planning, contract structure, and contract oversight.

Several DHS OEs have large, complex, high-cost procurement programs under way that need to be closely managed. For example, CBP's Automated Commercial Environment (ACE) project will cost $5 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost $17 billion and will take two to three decades to complete. Further, the department recently awarded a $10 billion contract for the development of a system to support the United States Visitor and Immigrant Status Indication Technology (US-VISIT) program for tracking and controlling the entry and exit of all aliens entering and leaving the country through air, land, and sea ports of entry. According to departmental officials, this program is on track to be implemented fully within the next ten years. Also, TSA's managed information technology services contract will cost over $1 billion. DHS OIG will be reviewing these major procurements on an ongoing basis.

GRANTS MANAGEMENT

DHS manages a variety of grant programs, totaling approximately $10 billion in obligations for 2003, which provide money for disaster preparedness, prevention, response, and recovery. Significant shortcomings have been identified in many of these programs in the past, including the potential for overlap and duplicate funding. In an effort to achieve better coordination, the Office for Domestic Preparedness and Office of State and Local Coordination were consolidated into the Office of State and Local Government Coordination and Preparedness (SLGCP). That office is responsible for 25 preparedness grant programs, including first responder grants.

However, much work remains to be done. In March 2004, the OIG issued *An Audit of Distributing and Spending "First Responder" Grant Funds, OIG-04-15.* The report identified problems at the state and local level that were causing grant fund distribution and spending to be slow. The problems included too many large grant programs that had to be processed in too short a time with inadequate state and local staffing; a lack of federal guidance on preparedness standards; complex and time consuming state and local planning processes; and burdensome state and local procurement and grant approval processes. The department is taking action to minimize state and local governments' problems and provide

more assistance. For example, DHS developed a grants management technical assistance program for state and local grantees.

On March 15, 2004, Secretary Ridge formed the Task Force on State and Local Homeland Security Funding to examine why federal funds were not reaching local governments and first responders in a timely fashion. In June 2004, the Task Force issued its report, and DHS officials said that it is incorporating the recommended actions in the Task Force report to produce measurable progress in grant fund distribution and spending.

The OIG is currently conducting audits of individual states' management of first responder grants and analyzing the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. The OIG will continue its audits of the department's disaster relief programs, and, in FY 2005, will conduct audits of state and local governments' use of first responder grant funds.

In assessing DHS grant management operations, the advice of the 9/11 Commission is pertinent. It recommended, "[F]ederal homeland security assistance should not remain a program for general revenue sharing. It should supplement state and local resources based on the risks or vulnerabilities that merit additional support."[1] In the OIG's recent draft report on the DHS Port Security Grant program, the OIG reported that DHS grant making for this sector of national infrastructure was not well coordinated with the IAIP Office of Infrastructure Protection, did not account for infrastructure protection priorities in the application review process, and resulted in funding of projects with low scores in the review process. Also, the DHS does not have a strong grant evaluation process in place by which to address post-award administration issues, including measuring progress in accomplishing DHS' grant objectives.

Department officials note that SLGCP, the United States Coast Guard, the Department of Transportation's Maritime Administration (MARAD), and TSA are partners in the Request for Application development as well as the evaluation panels for the Port Security Grant Program. As the lead agency for port security, the United States Coast Guard has been working with IAIP on port-wide criticality assessments. The Port Security Grant Program requires applicants to have completed a security vulnerability assessment as required in the Maritime Transportation Security Act (MTSA). The United States Coast Guard has defined the criteria for the structure of the required vulnerability/risk assessments under MTSA. Department officials said that in FY 2005, SLGCP will involve IAIP's Office of Infrastructure Protection appropriately in the Port Security Grant Program.

Department officials also said that staffing is inadequate to supporting the administration of the Port Security Grant Program's post-award phase. Staff developed a report to be submitted by the grantee at the end of the project period. This data will provide broad statistics demonstrating how the grant award funding has reduced the grantees' risk as identified by their security vulnerability assessment. Department officials said that in FY 2005, SLGCP plans to increase staff to allow for site visits and improved oversight of grant-funded projects.

[1] Final Report of the National Commission on Terrorist Attacks upon the United States, page 396 (2004).

FINANCIAL MANAGEMENT

Integration and Reporting

In March 2004, the department issued its first *Performance and Accountability Report* (PAR), containing its first set of published financial statements. The department received a qualified opinion on its balance sheet as of September 30, 2003, and the statement of custodial activity for the seven months then ended. This was a significant accomplishment for a large and complex department that was just starting-up. This effort produced a baseline for improvement with identification of 14 reportable conditions, seven of which were considered to be material weaknesses.[2]

The material weaknesses consisted of control weaknesses in the following areas:

A. Financial Management and Personnel
B. Financial Reporting
C. Financial Systems Functionality and Technology
D. Property, Plant, and Equipment
E. Operating Materials and Supplies
F. Actuarial Liabilities
G. Transfers of Funds, Assets, and Liabilities to DHS

The other reportable conditions consisted of control weaknesses in these areas:

H. Drawback Claims on Duties, Taxes, and Fees
I. Import Entry In-bond
J. Acceptance and Adjudication of Immigration and Naturalization Applications
K. Fund Balance with Treasury
L. Intra-governmental Balances
M. Strategic National Stockpile
N. Accounts Payable and Undelivered Orders

The department had very little time to focus on correcting the above deficiencies before the start of the FY 2004 audit. Therefore, most material weaknesses and reportable conditions will carry forward into the FY 2005 audit report. The material weakness associated with transfers of funds, assets, and liabilities to DHS was specific to DHS' first reporting period and will not be carried forward. In August 2004, the Strategic National Stockpile was transferred to the Department of Health and Human Services and is no longer the

[2] Specifically, the American Institute of Certified Public Accountants define reportable conditions as "matters coming to the auditors' attention relating to significant deficiencies in the design or operation of internal controls that, in the auditors' judgment, could adversely affect the department's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements." Material weaknesses are defined as "reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions."

responsibility of DHS. Finally, the Secret Service resolved its material weakness regarding actuarial liabilities.

In FY 2004, the department faced reporting problems stemming from the reorganization of the former Immigration and Naturalization Service (INS) and the U.S. Customs Service into three new bureaus -- Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP), and U.S. Citizenship and Immigration Services (USCIS), referred to as the "tri-bureaus" – and the consolidation of accounting services for many small programs from outside of DHS into ICE. However, the department and ICE did not prepare a thorough, well-designed plan to guide the transition of accounting responsibilities within ICE. ICE fell seriously behind in the performance of basic accounting functions, such as account reconciliations and analysis of abnormal balances. The pervasiveness of errors in ICE's accounts will prevent the auditors from completing their work at ICE for the FY 2004 DHS financial statement audit.

At Coast Guard, the auditors will not be able to complete audit work this year on all accounts because of difficulties encountered. These difficulties will result in additional material weaknesses that will be reported in the upcoming FY 2004 audit report.

The department also faces a structural problem in its financial management organization. The bureaus control most of DHS' accounting resources, but the DHS Chief Financial Officer (CFO) has responsibility for DHS' consolidated financial reporting, which is dependent on those resources. Although coordination mechanisms are in place, monitoring controls at the DHS CFO's level are insufficient to ensure the accuracy of consolidated financial information. The seriousness of the material weaknesses and reportable conditions at DHS demands strong DHS CFO oversight and controls.

In October 2004, the President signed the Department of Homeland Security Financial Accountability Act (Act), a law that will significantly challenge the department's managers. The Act will require the department to make an assertion as to the effectiveness of its internal control structure beginning in FY 2005. In addition, proposed changes to OMB's Circular A-123 would require substantial agency resources and efforts to comply with the Circular's internal control documentation and reporting requirements. To complete this task, the department's financial managers will need to identify and document existing processes related to financial reporting, then perform their own testing of the design and effectiveness of internal control mechanisms and procedures. This requirement, similar to that levied on publicly traded companies under the Sarbanes–Oxley Act, goes far beyond any previous management review of internal controls over financial reporting performed by DHS. DHS will have to ensure that it complies with all standards of the Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* in order to achieve a clean audit opinion on internal control over financial reporting in FY 2006.

Revenue Collection

Annually, CBP collects more than $22 billion in duties, excise taxes, fines, penalties, and other revenue. CBP has had an active program to monitor trade compliance, but in the face

of critical homeland security responsibilities, counter-terrorism activities have begun to claim a higher share of border resources. CBP faces a challenge in protecting trade revenue and enforcing trade laws at a time when the terrorist threat demands much more from CBP's border resources.

CBP is responsible for collecting user fees from air passengers arriving in the United States. The fees are designed to offset the costs of inspection services provided by CBP, which now includes the former INS and the Animal and Plant Health Inspection Service (APHIS) inspection processes. Between FYs 1998 and 2002, the former U. S. Customs Service collected $1.1 billion from the airlines. Now that CBP's inspection workforce has expanded to include the former INS and APHIS inspection services, it is important that CBP ensure that revenues collected are accounted for and are adequate to cover the costs of services provided. In addition, the TSA is required to impose a fee on airline passengers. This fee is designed to offset the costs of providing civil aviation security services provided by screening personnel, Federal Air Marshals, and equipment. The OIG and GAO are currently auditing the collection of airline passenger fees.

USCIS generates more than $1 billion in revenues through collection of immigration and naturalization application fees from non-citizens seeking entry into the United States. In fulfilling its mission, USCIS processes millions of actions and requests that are documented in paper files. The systems that track these applications are not integrated, and many are *ad hoc*. Deferred revenue is a financial measure of pending applications and is material to DHS' financial statements. The challenge for USCIS is to move from paper based and non-integrated processes to an integrated case management system.

HUMAN CAPITAL MANAGEMENT

The Homeland Security Act gave DHS special authorization to design a human capital management system that fits its unique missions. On April 1, 2003, the department announced that it would assemble a team of diverse employees from across the department and representatives from OPM and major unions to design a new human capital management system for the department's approximately 180,000 employees. This team developed a range of options for pay and classification, performance management, labor relations, discipline, and employee appeals that were presented to the Secretary and the Director of OPM. The decisions of the Secretary and the Director were published as proposed regulations and public comments were received. DHS received over 3,500 comments from employees, DHS employee unions, the general public, and members of Congress during the public comment period. DHS spent four weeks with major DHS employee labor union representatives in congressionally mandated "meet-and-confer" sessions and then extended that process for an additional two weeks. Secretary Ridge and Director James personally met with the presidents of the two largest DHS employee labor unions in early September 2004. DHS continues to carefully review and consider the issues raised in those forums. Once that review is completed, department officials say that it will move forward with a new human resource management system that will support the mission of the Department of Homeland Security while recognizing the rights of its employees. According to the department, these

new regulations will dramatically affect not only DHS employees, but also, at least potentially, the entire civilian workforce, as the DHS system will likely be considered a model for civilian personnel programs government-wide. In June 2004, the department awarded a contract for services related to the development and implementation of a new human resource system, MAXHR.

An additional serious problem involves the length of time necessary to complete the security clearance process, even for federal employees from other agencies who hold clearances when they enter DHS. At the same time, several OIG reviews have noted flaws in the background investigations of new employees, notably the reviews of TSA's screeners and the Federal Air Marshals Service. The OIG does not advocate a reduction of diligence in the personnel security process, but notes that the delays are long and have adversely affected DHS' operations.

INTEGRATION OF INFORMATION SYSTEMS

Creating a single infrastructure for effective communications and information exchange remains a major management challenge for DHS. To meet this challenge, the chief information officer (CIO) has efforts under way to determine the strategies and technologies needed to connect the local, metropolitan, and wide area networks of the department's legacy agencies. Specifically, DHS enhanced the ICE's telecommunications "backbone" to create the department-wide network, establishing data communications for the establishment of the department's initial capability. Subsequently, a new concept has been developed and an initiative is under way to create the department-wide network that will establish common policies and technical standards for data communications among all organizational components. Further, the CIO is working with line managers to complete a second version of enterprise architecture to guide management of information and technology in the department. The CIO released the first version of the architecture in September 2003, and is now working to make its transition strategy more detailed and easier to implement and align with several of DHS' large information technology (IT) projects. Additionally, DHS has established the "eMerge^{2}" program,[3] scheduled for implementation by September 2006, to integrate the redundant and nonintegrated systems used to support administrative activities such as accounting, acquisition, budgeting, and procurement.

However, as the OIG reported in July 2004, the DHS CIO is not well positioned to meet the department's IT objectives. Despite federal laws and requirements, the CIO is not a member of the senior management team with authority to strategically manage department-wide technology assets and programs. No formal reporting relationship is in place between the DHS CIO and the CIOs of major component organizations, which hinders department-wide support for his central IT direction. Further, the CIO has limited staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support departmental units. These deficiencies in the IT organizational structure are exemplified by the CIO's lack of oversight and control of all DHS' IT investment decision-

[3] Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency (eMerge^{2}).

making and a reliance instead on cooperation and coordination within DHS' CIO Council[4] to accomplish department-wide IT integration and consolidation objectives. The department would benefit from following the successful examples of other federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on department-wide IT investments and strategies.

SECURITY OF INFORMATION TECHNOLOGY INFRASTRUCTURE

The security of IT infrastructure is a major management challenge. As required by the Federal Information Security Management Act (FISMA), the CIO must develop and implement a department-wide information security program that ensures the effectiveness of security controls over information resources that address the risks and vulnerabilities facing DHS' IT systems.

As DHS OIG reported in September 2004, based upon its annual FISMA evaluation, DHS has made significant progress over the last year in developing, managing, and implementing its information security program at the departmental level. The Chief Information Security Officer (CISO) updated many of its IT security policies and procedures and together, these policies and procedures, if fully implemented by the components, should provide DHS with an effective information security program that complies with FISMA requirements.

Even though DHS has made several improvements in its information security program, the OEs have not yet fully aligned their respective security programs with DHS' overall policies, procedures, and practices. For example, DHS cannot effectively manage its information security program while lacking an accurate and complete system inventory. The CISO has developed a formal inventory methodology based on federal guidance including FISMA and National Institute of Standards and Technology publications. Currently, the CISO has a team visiting OEs to facilitate inventory alignment based on the methodology. Further, as reported in our FY 2003 security program evaluation, DHS' OEs are not ensuring that IT security weaknesses are included in their Plan(s) of Action and Milestones (POA&M). To address this issue the CISO has implemented POA&M assist visits with each of the OEs, to better manage the entire POA&M process, including the identification and management of all security weaknesses.

In a separate report issued by the DHS OIG in June 2004, security controls were found to be inadequate and increase the risks to DHS wireless networks. The DHS OIG reported issues with wireless policy, procedures for wireless implementation, and effective oversight by DHS' National Wireless Management Office (WMO). The DHS WMO is working closely with the CISO to ensure that wireless security policy is properly formulated and promulgated, and is sufficient to ensure DHS' wireless communications. Department officials said that it will implement and maintain a rigorous certification and accreditation

[4] The DHS CIO Council is comprised of the CIOs from each DHS component, ex officio representatives from General Counsel, the Chief Financial Officer's Council, the Office of the CIO, and the Executive Procurement Executive Council. The CIO Council was chartered to develop, promulgate, implement, and manage a vision and direction for information resources and telecommunications management within DHS.

(C&A) process for all wireless systems, personal electronic devices, and tactical wireless communication systems. Specifically, the Wireless Security Working Group within DHS will coordinate with the DHS WMO and DHS CISO to ensure consistency in the development and application of risk management approaches and C&A processes for wireless services and technologies. Department officials also said that this collaboration ensures the DHS WMO is effectively managing the department's wireless security risks. Additionally, the Designated Accrediting Authority within each organizational component will be responsible for approving the implementation and use of wireless systems at a specified risk level during the C&A process.

The department is also tasked to protect the nation's critical infrastructure from a major cyber terrorist attack. The DHS OIG reported in July 2004 that DHS has begun to implement the actions and recommendations detailed in *The National Strategy to Secure Cyberspace*. While a number of major initiatives have been undertaken, DHS still faces many challenges to address long-term cyber threats and vulnerabilities to the nation's critical infrastructure.

INFRASTRUCTURE THREAT ASSESSMENT

The department is tasked to protect the nation's critical infrastructure and national assets against terrorist attack. Before this assignment can be executed to its fullest, the IAIP directorate must identify and then compile the nation's critical infrastructure and national assets into a comprehensive National Assets Database (NADB). DHS has made progress on this task; as of July 2004, the NADB contained more than 33,000 national assets. However, the process the IAIP is using to assess the threats against those assets, determine how vulnerable they are to attack, ascertain their mitigation requirements, and prioritize the threat/mitigation effort is evolving. Presently, there is no blueprint for the NADB as no precedent exists for collecting such extensive information and making these difficult qualitative and quantitative assessments. Policies and procedures for maintaining the NADB are still in development. Although the IAIP provided guidance for the collection of data, the data it received was often inconsistent. The DHS OIG is evaluating the effectiveness and efficiency of the processes that the IAIP employs to develop and prioritize its inventory of the nation's key assets.

BORDER SECURITY

A primary mission of the DHS is to reduce America's vulnerability to terrorism by protecting the borders of the United States and safeguarding its transportation infrastructure. Within DHS, these responsibilities fall primarily with the Border and Transportation Security (BTS) Directorate.

Two organizations within BTS are responsible for enforcing the nation's immigration and customs laws. CBP inspects visitors and cargoes at the designated U.S. ports of entry (POE) and is responsible for securing the borders between the POEs. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the United States, while also

facilitating the flow of legitimate trade and travel. ICE is the investigative arm of BTS that enforces immigration and customs laws within the United States. While CBP's responsibilities focus on activities at POEs and along the borders, ICE's responsibilities focus primarily on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the United States, regardless of where the violation occurs. CBP and ICE have employees assigned outside the United States to protect the sovereignty of our borders.

Other organizations within DHS have border security related responsibilities. For example, the US-VISIT Program Office, also within BTS, is responsible for the development and fielding of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). Also, USCIS is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS plays an integral part in DHS' border security program by ensuring that only eligible aliens receive immigration benefits and identifying cases of immigration benefit fraud and other immigration violations that warrant investigation or removal by ICE.

DHS faces several formidable challenges in securing the nation's borders. These include the development of an effective, automated entry-exit system (US-VISIT); disruption of alien smuggling operations; identifying, locating, detaining, and removing illegal aliens; fielding effective border surveillance technologies; integrating DHS' IDENT with the FBI's IAFIS fingerprint systems; providing timely, accurate, and complete intelligence to support border security operations; developing effective overseas operations; and, reducing the immigration benefit application backlog.

Tracking the Entry and Exit of Foreign Visitors

US-VISIT will provide the capability to record entry and exit information on foreign visitors who travel through United States air, sea, and land ports, and it will apply to non-immigrants holding non-immigrant visas. DHS thinks that the US-VISIT program will take five to ten years to implement fully its long term, comprehensive vision. To support US-VISIT in meeting its challenge, the US-VISIT Program Office awarded the prime integrator contract on June 1, 2004. The initial five-year contract, with one-year options for extension of another five years, is worth up to $10 billion. Managing this mammoth project and associated budget will require considerable management and contractor oversight by DHS. The project has considerable risk, not only in terms of technology challenges that must be overcome, but the end product of the project is still undefined.

Alien Smuggling

Alien smuggling continues to be a major immigration problem in the United States. As border enforcement operations have made illegal entry into the United States more difficult, smugglers have profited. In addition to boosting their fees, smugglers have become

increasingly dangerous and aggressive in their tactics. ICE faces significant challenges in curbing these sophisticated and dangerous smuggling operations. ICE's limited resources have always been strained in its attempts to counter the economic magnet of the U.S. employment market. ICE reports that its Arizona Border Control Initiative led to a decrease in smuggling activity, the seizure of over $5.3 million in smuggling assets, and the confiscation of 130 firearms.

Identifying, Locating, Detaining, and Removing Illegal Aliens

DHS continues to face challenges in identifying, locating, detaining, and removing aliens who have entered without inspection, violated the terms of their visas, or committed criminal acts. The current illegal alien population in the United States is estimated to be 8-12 million. ICE, the agency responsible for removing the illegal alien population, continues to wage an uphill battle to address this problem. ICE is hampered in part by shortages of special agents. It has approximately 5,500 special agents to cover the myriad of immigration and customs law enforcement responsibilities, of which locating illegal aliens is but one. ICE utilizes DHS non-immigrant registration systems, including the National Security Entry Exit Registration System (NSEERS), the Student and Exchange Visitor Information System (SEVIS), and US-VISIT to assist in the process of identifying and locating visa overstays and student status violators.

Further, ICE has the responsibility to detain certain illegal aliens until they are removed from the United States. With increasing frequency, ICE has been forced to weigh its detention decisions against budgetary constraints. Prior reports have shown the importance of detention in relation to the eventual removal of an alien. Hence, effective management of BTS detention space can substantially contribute to immigration enforcement efforts.

Advanced Border Surveillance Technology

CBP is challenged to monitor illegal immigration activity along remote and rugged stretches of the U.S. border with Mexico and Canada. Even if additional Border Patrol agents were available, officers alone cannot effectively monitor some border regions. CBP has employed technology to enhance border surveillance and its ability to detect illegal immigration activity. The technology includes the American Shield Initiative (ASI) and unmanned aerial vehicles. The challenges for CBP are to identify effective technologies; deploy the technologies appropriately; and integrate effectively those technologies as "force multipliers" into its border enforcement strategy.

Integrated Fingerprint Systems

DHS must move rapidly to complete the deployment of the integrated IDENT/IAFIS workstations to the border. Immigration authorities have long recognized the need for an automated fingerprint identification system to determine quickly the immigration and criminal histories of aliens apprehended at or near the border. Immigration authorities need to be able to determine quickly which aliens should be detained for prosecution based on membership in a terrorist organization, multiple illegal entries, re-entering the United States

after a prior deportation, alien smuggling, a current arrest warrant, or an aggravated criminal record.

In FY 1989 Congress provided the initial funding to develop an automated fingerprint identification system that eventually became known as IDENT. While IDENT was developed to meet identification purposes, the FBI developed its own fingerprint system, IAFIS, to meet its own requirements. Beginning in 1998, the need to integrate the two systems was recognized. IDENT could not interface with the FBI's fingerprint system, which prevented immigration authorities from obtaining criminal histories of aliens they had in their custody. In FY 1999, Congress mandated the integration of IDENT and IAFIS. The Department of Justice (DOJ) was originally given the responsibility for integrating the systems and was funded through annual appropriations. In FY 2004, despite not receiving funding, DHS was given responsibility for continuing the deployment of the IDENT/IAFIS capability. In addition, FY 2005 appropriations language tasks DHS to take the lead on future development of any integrated IDENT/IAFIS capability. DHS will be required to submit a report on the status of this effort, including steps the department will take to integrate IAFIS into IDENT, funds needed, and a timetable for full integration.

The integration project was started in 2000 with studies to be performed by DOJ on the impact of deploying an integrated IDENT/IAFIS capability. The first published schedule called for a limited integrated capability to be developed and deployed to selected sites by late 2002. Various delays and changes in project scope pushed out DOJ's schedule. Only a small percentage of sites had the capability by the beginning of FY 2004. To date, initial integrated workstations exist at all Border Patrol locations and most of the major ports of entry. Department officials said that the integrated workstation will allow a field agent to take a single set of fingerprints and simultaneously query both IDENT and IAFIS in real time, and that deployment to the remaining POEs and all interior locations should be completed in 2005.

The DOJ OIG reported in January 2004 that all aliens apprehended by the Border Patrol still are not checked against FBI criminal fingerprint records. Additionally, the FBI and other law enforcement agencies using the FBI's fingerprint records still cannot access DHS' criminal alien fingerprint records. The transfer of immigration responsibilities to DHS has created additional issues relating to the management of the integration project between DHS and DOJ. According to the DOJ OIG, unresolved issues include: (1) project leadership and responsibilities between DHS and DOJ; (2) funding; (3) technical interoperability issues between US-VISIT and IAFIS; (4) the development of integration project schedules; and (5) fingerprint image quality concerns.

Intelligence Support for Border Security Operations

Integrating the multiple data systems to compile a complete border security picture without requiring queries of multiple systems by ICE and CBP officers will be a major challenge. In order for CBP and ICE officers to identify potential threats to the security of the United States, whether it be persons or cargoes, they must be able to access all relevant information and intelligence from all sources regarding persons, vehicles, vessels, aircraft, criminal histories, travel records, etc. Officers must be able to access quickly information to develop

a complete picture of the current border security situation so that they can make appropriate enforcement decisions. Quick access to information is also vital to CBP's objective of facilitating legitimate travel and trade. However, officers must now conduct time consuming and difficult multiple database searches because systems are not integrated. The systems that they use are antiquated and not easily operated. Data displays are not always clear and officers could miss or overlook important information. Data within the systems cannot always be manipulated to conduct in-depth analysis to discern trends and patterns of illegal activities.

Efforts are currently ongoing to consolidate the various terrorist watch list systems used by federal agencies, and thereby help improve intelligence support for border security operations. According to the Homeland Security Act of 2002, DHS is to play a major role in watch list consolidation activities. However, these consolidation activities are still conducted by the federal organizations that were primarily responsible for collecting and disseminating terrorist information prior to DHS' formation.

International Operations

DHS faces international challenges in protecting our borders. Provisions in the visa issuance process and other programs to promote international travel create potential security vulnerabilities that may allow terrorists, criminals, and other undesirable travelers to enter the United States undetected.

For example, DHS must address security concerns identified in the Visa Waiver Program (VWP). The VWP enables citizens of 27 countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. These travelers are inspected at a U.S. POE, but have not undergone the more rigorous background investigations associated with visa applications.

BTS needs to strengthen and improve the management of the VWP, including issues related to lost and stolen passports (LASP). LASP information provided by VWP governments has not been thoroughly checked by the former INS or now by BTS against U.S. entry and exit information to determine whether the passports have been used to enter the United States. Collection of LASP data from VWP governments is not proactive or uniform. Further, LASP problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *male fide* (in bad faith) travelers using stolen VWP passports even when the theft has been reported. The OIG recommended that US-VISIT biometric processing be extended to VWP travelers, a program change that DHS has adopted.

DHS must also address issues identified with its visa security program (VSP). The VSP stations DHS officers at U.S. embassies and consular offices overseas to review visa applications and perform other law enforcement functions. The VSP program received partial funding in FY 2004 and full funding in FY 2005. Because BTS has been compelled to use temporary duty officers who have not received training in foreign languages, they do not have these skills, and lacked adequate administrative support as well. As a result, the full

intelligence and law enforcement value that Visa Security Officers could add to the existing inter-agency country teams has not been achieved.

CBP has started a new program, the Immigration Security Initiative (ISI), to station CBP officers in foreign airports. The ISI officers are to interdict terrorists, illegal aliens, alien smugglers, and other criminals before they board U.S.-bound flights. As with any new initiative, CBP is faced with several challenges in establishing and managing this new program. First, adequate funding must be provided. Second, the officers working in the foreign airports must have adequate technical and administrative support to perform their missions. This includes connectivity to electronic database systems, which could be problematic in a foreign facility. Third, CBP must develop a cadre of specially trained officers that it can rotate into these positions.

Immigration Benefit Application Backlog Reduction

USCIS is challenged with processing immigration benefit applications and petitions in a timely manner. As of May 2004, USCIS had pending 5,696,066 applications and petitions. Of these, 233,696 were for asylum; 671,707 for naturalization; and 4,790,663 for immigration benefits. The Administration announced the aim of meeting a six-month standard from start to finish for processing applications for immigration. The President pledged $500 million over five years, beginning with $100 million requested for fiscal year 2002, to support USCIS in eliminating the backlog by the end of 2006.

USCIS issued a "Backlog Elimination Plan" in June 2004 that reframed how USCIS counts the backlog and proposed the following backlog elimination strategies: (1) new management tools; (2) improved processes and procedures; and (3) better use of technology. USCIS' backlog reduction plan is ambitious and is based on numerous assumptions about application receipts, increased productivity, and the success of some pilot programs currently being conducted. Many of these assumptions would be severely disrupted if global immigration patterns or U.S. immigration law encountered significant changes. For example, a proposed new guest worker program would permit many currently illegal aliens to apply for some form of immigration status. If USCIS were suddenly inundated with potentially millions of unexpected immigration benefit applications, its efforts to eliminate current backlogs would be severely hindered.

TRANSPORTATION SECURITY

Airport Screeners

The Aviation and Transportation Security Act (ATSA), which was enacted as a result of the events of September 11, 2001, mandated that the TSA hire and train thousands of screeners for the nation's 429 commercial airports by November 19, 2002. As a result, TSA hired 62,000 screeners. A DHS OIG undercover audit of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports or do not enter the checked

baggage system. Four areas caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs along with management and supervision of screener activities. The DHS OIG is evaluating TSA's revised training programs and will continue to monitor TSA's progress in improving screeners' performance.

Checking for Explosives

TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems (EDS). However, deployment of the equipment does not ensure effective security. Several OIG reviews have reported that TSA has not resolved the problems that arise when explosive detection equipment breaks down, there are workforce shortages, or high baggage volume overloads the system. Fallback alternatives are inconsistently applied and inadequately controlled, leaving gaps in the screening process. Also remaining to be done are: (1) deploying such equipment to the remaining airports where alternative screening methods are in use today; (2) integrating explosives detection systems into baggage handling systems at the largest airports (at a cost of more than $3 billion); and, (3) using research and development funds to develop and deploy more effective and economical equipment to address current and future threats and risks. Additional safeguards are also needed to screen and inspect cargo transported on passenger aircraft.

Recently, TSA has come under criticism from both members of Congress and the 9/11 Commission for not moving quickly enough to address the vulnerability of the nation's air traffic to suicide bombers. Specifically, TSA has not installed explosives detection technologies at the checkpoint to screen for explosives on the body. TSA is in the process of testing several of these technologies that include backscatter x-ray, vapor detection, and document scanner machines to address concerns regarding detection of explosives on individuals. TSA is currently piloting explosives trace detection document scanners at four airports to assess the viability and effectiveness of the technologies.

DHS OIG is continuing to monitor TSA's progress regarding these issues as well as reviewing TSA's process for screening air cargo.

Maritime Security

The U.S. Coast Guard is the lead DHS agency for maritime homeland security, and is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. The marine areas under U.S. jurisdiction cover 3.5 million square miles of ocean, 95,000 miles of coastline, and 26,000 miles of commercial waters serving 361 domestic ports. These activities account for two billion tons and $800 billion of domestic and international freight annually. Approximately 8,000 foreign vessels, manned by 200,000 foreign sailors, make more than 50,000 ship visits to U.S. ports each year.

The Coast Guard faces significant management challenges. The most daunting challenges include restoring the Coast Guard's readiness to perform its legacy missions; implementing the Maritime Transportation Security Act of 2002 (MTSA); maintaining and replacing the Coast Guard's deepwater fleet assets; and developing adequate infrastructure needed to support the Coast Guard's multiple missions.

Readiness to Perform Coast Guard Legacy Missions

The Coast Guard faces three major barriers to improving and sustaining its readiness to perform its legacy missions. First, the lack of a comprehensive and fully defined performance management system impedes the Coast Guard's ability to gauge its performance, allocate resources effectively, and target areas for improved performance. The Coast Guard has yet to comprehensively define a performance management system that includes all the input, output, and outcomes needed to gauge results and target performance improvements, balance its missions, and ensure the capacity and readiness to respond to future crisis or major terrorist attacks. Second, the workload demands on the Coast Guard will continue to increase as it implements MTSA. This complex work requires experienced and trained personnel; however, the Coast Guard has in recent years suffered from declining experience levels among its personnel. Third, sustaining a high operating tempo due to growing homeland security demands, such as added port, waterway, and coastal security patrols, will tax the Coast Guard's infrastructure including its aging cutter and aircraft fleet.

Implementing MTSA

The Coast Guard faces challenges in fully implementing MTSA and enforcing the required vessel, facility, and area security plans. MTSA regulations affect approximately 9,200 vessels, 3,200 port facilities, and 40 offshore terminals. Owners and operators of vessels, facilities, and terminals were required to develop port security plans consistent with Area Maritime Security Plans. Vessel and facility plans were reviewed and approved by the Coast Guard, and implemented by July 1, 2004. The Coast Guard, working through Captains of the Port, is working to develop and implement 43 Area Maritime Security Plans covering the Nation's 361 seaports. These plans are to be implemented in concert with the national security and homeland defense strategies and plans. The Coast Guard must ensure that these plans are effectively implemented, including its key and unique role of ensuring the MTSA regulations are enforced.

In addition, the Coast Guard must identify, target, track, board, inspect, and escort high interest vessels that may pose a substantial risk to U.S. ports due to the composition of the vessel's crew, passengers, or cargo. The Coast Guard has instituted strict reporting requirements for all vessels arriving at U.S. seaports, mandating most commercial vessels to provide a 96-hour Advance Notice of Arrival. Certain vessels operating on U.S. navigable waters must also be equipped with and operate an Automatic Identification System (AIS), which includes a position indicating transponder. The Coast Guard has also developed a sophisticated decision-making system for targeting high interest vessels, cargoes, and crews. The Coast Guard faces a major management challenge to validate and fully implement these targeting procedures.

Maintaining and Replacing Deepwater Assets

In June 2002, the Coast Guard awarded a $17 billion contract to maintain and replace its Deepwater assets. This contract called for replacing or modernizing, by 2022, all assets used in missions that primarily occur more than 50 miles offshore, including approximately 90 cutters, 200 aircraft, and assorted sensors and communications systems. According to the Coast Guard, the greatest threat to its ability to safely and effectively perform its assigned missions continues to be the operational capability of its legacy aircraft, cutter, and small boat fleet. These assets are aging and are becoming more difficult and expensive to maintain. In some instances, the Coast Guard is experiencing difficulty maintaining and upgrading existing critical deepwater legacy assets including the HH-65, HH-60, HC-130 aircraft and its coastal patrol boat fleets.

Maintaining the operational readiness of critical legacy assets is a major challenge to the Coast Guard. As an example, the rate of in-flight loss of power mishaps involving the HH65 helicopter far exceeds FAA and U.S. Navy safety standards, requiring the immediate re-engining of the entire HH65 fleet. The Coast Guard estimates that sustaining its deteriorating legacy assets will escalate to $140 million in fiscal year 2005, further challenging the Coast Guard to rethink plans and schedules for maintaining or replacing legacy assets.

Revisiting maintenance, upgrade, and replacement decisions for legacy assets may disrupt the Deepwater contractor's plans and schedules and, therefore, could greatly increase future program costs. For example, the Coast Guard must diligently monitor the schedule and costs for maintaining, renovating, or upgrading its coastal patrol boats and medium and high endurance cutters. Revisiting these decisions may be prudent, considering the adverse impact deteriorated fleet conditions are having on Coast Guard mission performance. In 2003, the Coast Guard experienced 676 unscheduled maintenance days for its cutters—a 41% increase over 2002. This was the equivalent of losing the services of over three and a half cutters. These lost cutter days include the coastal patrol boats that are suffering from accelerated hull corrosion and breached hull casualties.

Infrastructure in Support of Coast Guard Missions

The Coast Guard Acquisition, Construction, and Improvement (AC&I) budget requests during FY(s) 2003-2005 did not include adequate funding for the re-capitalization of critical infrastructure. For example, the Coast Guard requested only $5.5 million for shore side infrastructure during FY 2004. This infrastructure must be planned, designed, funded, and constructed in time to support properly the Deepwater boats, cutters, and aircraft, as well as their crews. The lack of infrastructure funding could be a major detriment to the Coast Guard's ability to perform both its legacy and homeland security missions.

Other Transportation Modes

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across the other modes of transportation. About 6,000 agencies provide

transit services through buses, subways, ferries, and light-rail services to about 14 million Americans. Recently, several congressional leaders expressed concern that the federal government has not taken strong enough action to respond to the threat to passenger and public transit. Furthermore, the 9/11 Commission recently reported that over 90% of the nation's $5.3 billion annual investment in TSA goes to aviation, and that current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits so that transportation security resources can be allocated to the greatest risks in a cost effective way.

TSA has lead responsibility for coordinating development of a transportation sector plan, which should be completed by the end of the year. TSA, however, has not finalized the memorandums of understanding with various Transportation Department agencies to determine how they will coordinate work in the future.

DHS OIG is evaluating TSA's actions to assess and address potential terrorist threats to the mass transit systems of major U.S. metropolitan areas.

Management's Response to the Inspector General's Statement on the Top Management Challenges Facing the Department of Homeland Security

The Department recognizes the challenges identified by the Inspector General (IG) and the potential impact the challenges could have on the effectiveness and efficiency of department programs and operations if not properly addressed. In most cases, the IG's statement identifies the priority actions the Department is taking to address these challenges, many of which have been completed or are currently in progress. This is especially so in light of the fact that the fieldwork associated with the Office of the Inspector General (OIG) Report's underlying reviews was completed many months ago. The Department anticipates that the results of initiatives to address the management challenges during fiscal year 2005 and a reassessment of other challenges should enable the IG to report formidable progress next year. Some challenges, however, require legislative action or necessitate that actions be taken jointly with non-Department of Homeland Security government agencies.

Where a sustained effort is required over several years to address an OIG management challenge that impacts a core program or management priority, performance goals and strategies will be developed at either the Departmental or agency level and included in annual performance plans. For example, plans at the Departmental and agency level are in place to comprehensively address management challenges such as integrating information systems and issues on border and transportation security identified in the IG's statement. These long-term plans will be reflected in the Department's *Future Years Homeland Security Program*.

The following provides additional information to amplify or clarify the corrective actions identified in the IG report:

Consolidating the Department's Components

During the first 20 months of existence, the Department has accomplished the largest reorganization of the Federal Government in more than half a century. This task, creating the third largest cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented many challenges, which are being met by the Department's managers and employees. The Department recognizes there is yet much to be done and is taking those steps crucial to integrating and consolidating the various components of the Department.

The Department is integrating and streamlining the support service functions directly accountable to the functional Line of Business (LOB) Chiefs such as the Chief Procurement Officer (CPO), Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO) and Chief of Administrative Services (CAS). The LOB Chiefs have developed Management Directives to guide the Department's management of that business function and are now implementing systems to optimize their functions across the entire Department. The systems are based on "dual accountability" where both the operational leadership and the LOB chiefs are responsible for the successful implementation of the directives. The Management Directives provide direction for both process and resource management. The Secretary signed these documents in October to institutionalize the arrangements before fiscal year 2005.

Contract Management

Overall, the Department is taking positive steps to build and improve the Department's contract management system. To help address the issues raised by the OIG, the Department formed the Office of Procurement Operations (OPO) to provide procurement support for components without an indigenous contracting capability. To help bridge the staffing gap, the Department contracted with other federal agencies to provide contract management support. The OPO has developed a staffing plan to bring OPO's staffing level to 127 by the end of fiscal year 2005. The cost of these positions will be funded through the Working Capital Fund.

The Department's efforts to provide a sufficiently detailed and accurate listing of procurement information proved difficult and were hampered by legacy federal systems. While it has migrated all of its procurements under the umbrella of one comprehensive reporting system, the Department still lacks sufficiently detailed and validated data for fiscal year 2003 and fiscal year 2004 to manage the procurement universe and ensure accurate and consistent reporting.

To help ensure large, complex, high-cost procurement projects are closely and properly managed, the Department has implemented a vigorous Investment Review Process (IRP) that:

- Integrates capital planning and investment control, resource allocation, budgeting, acquisition, and management of information technology and non-information technology investments to ensure scarce public resources are wisely invested and operational requirements are met.
- Ensures that spending on investments directly supports and furthers the Department's mission and provides optimal benefits and capabilities to stakeholders and customers.
- Identifies poorly performing investments that are behind schedule, over budget, or lacking in capability so corrective actions can be taken.
- Identifies duplicative efforts for consolidation and mission alignment when it makes good sense or when economies of scale can be achieved.
- Improves investment management in support of the President's Management Agenda.

To date, over 75 percent of the Department's major investments have been reviewed by the Investment Review Board (IRB) or the Joint Requirements Council.

Financial Management

We acknowledge the significant financial management challenges facing the Department of Homeland Security and we are committed to work with the OIG to establish a world-class financial management program. Between our inaugural and second year of operations we have demonstrated resolve and have:

- Steadily improved the involvement of component level financial management resources.
- Hired a diverse set of financial management expertise in the areas of accounting systems, the U.S. Standard General Ledger, financial reporting, and internal controls.
- Partnered with private sector consultants to produce standard operating procedures that will promote consistent, timely, and accurate consolidated financial reporting in compliance with Federal accounting standards and control requirements.

We are firmly committed to accountability and embrace the *Department of Homeland Security Financial Accountability Act*. In fiscal year 2005, we will approach financial management "methodically; building our financial management infrastructure right is more important to us than rushing to an outcome." We are already proactively engaged in numerous activities to better our financial management processes. In fiscal year 2005 we will:

- Integrate financial management functions to achieve our goal of a functionally integrated Department.
- Continue to use public and private sector partnerships to prepare standard financial management operating policies and procedures. We are utilizing best-in-class financial management policies and procedures to assist in expediting our efforts in this area. This will set the financial management internal control framework for the Department.
- Launch implementation of a strategy to transform legacy internal control structures into a Departmental internal control structure.
- Conduct an operating risk assessment of our financial reporting processes. The assessment will provide a gap analysis to identify the key risks over Departmental financial reporting and an inventory of internal control issues to enable us to close control gaps.

The Office of the Chief Financial Officer (OCFO) is pursuing an efficient and integrated approach that builds on government, industry, and project management best practices for acquiring a commercial off-the-shelf financial management package and the system integration expertise necessary for implementation. This approach called eMerge^2 will use a performance-based acquisition strategy based on effective planning and requirements-gathering consistent with department information technology policy and system development life-cycle guidance. OCFO is managing eMerge^2 using critical components of earned-value management methods for program planning, reporting, and management. OCFO has also developed appropriate planning documents, emphasizing different aspects of the effort, to ensure that the acquisition and implementation of a modern financial management system is cost-effective, efficient and meets the Department's business, technical and compliance needs.

Integration of Information Systems

Creating a single infrastructure for effective communications and information exchange is a major management challenge for the Department. The CIO is developing the strategies and technologies needed to connect the local, metropolitan, and wide area networks of the Department's legacy agencies.

The Department's CIO is an integral member at each level of the information technology investment review process. The Department's CIO heads the CIO Council (comprised of all CIOs across the Department) and the Enterprise Architecture Board and is a key member of the IRB as part of the Department's IRP. The IRB is the executive review board that provides acquisition oversight of the Department's major investments. The IRB is the forum that provides senior management the proper visibility, oversight, and accountability for major investments whether they are information technology or non-information technology. It also serves as a forum for discussing investment issues and resolving problems requiring senior management attention.

Maritime Security

The Coast Guard continues to improve a robust mission program performance management system and readiness to perform legacy missions in close coordination with the Department and OMB on Program Assessment Rating Tool reviews and independent program evaluations. Further refinement of the Coast Guard's comprehensive performance management system will include alignment and measurement of activities that contribute to department and Coast Guard agreed upon outcomes. This will further enable the Coast Guard to gauge results and target performance improvement, balance its missions, and ensure the capacity and readiness to respond to future crisis or major terrorist attacks. Coast Guard leadership is also proactively engaged in periodic long-term scenario planning to foresee future needs. For example, the Coast Guard is preparing a comprehensive schedule that will include the current status of its Deepwater Project asset acquisition phases (such as concept technology and design, system development and demonstration, and fabrication), interim phase milestones (such as preliminary and critical design reviews, installation, and testing), and the critical paths linking the delivery of individual components to particular assets.

The Coast Guard, in coordination with its industry partner, Integrated Coast Guard Systems, is analyzing repair or replace decisions for some assets. These analyses are being conducted primarily to ensure that the Coast Guard achieves operational requirements and does not suffer reduced asset capability. Additionally, an increase in cost is not necessarily a result. In some cases proposed changes will result in savings.