DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Major Management Challenges Facing the Department of Homeland Security

(Excerpts from the FY 2005 DHS Performance and Accountability Report)

Office of Audits

OIG-06-14

December 2005

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, and special reports prepared as part of our DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

The attached report presents the major management challenges facing the Department of Homeland Security and also was included in DHS' FY 2005 *Performance and Accountability Report*. As required by the Reports Consolidation Act of 2000, we update our assessment of management challenges annually.

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

Richard L. Skinner

Richard L. Skinner
Inspector General

Office of Inspector General

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

Homeland
Security

October 25, 2005

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

Since its inception in March 2003, 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.

We identified "major management challenges" facing the Department, as discussed below. These challenges are a major factor in setting our priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, we update our assessment of management challenges annually.

DISASTER RESPONSE AND RECOVERY

On August 29, 2005, Hurricane Katrina hit the Gulf Coast states of Louisiana, Mississippi, Alabama, and Florida, causing catastrophic damage to the region. By September 9, 2005, the Congress had passed legislation that provided $63 billion for disaster relief, the bulk of which went to the Federal Emergency Management Agency (FEMA). FEMA, in turn, tasked other federal departments and agencies through Mission Assignments and grants to affected states to assist with recovery efforts. Initial FEMA mission assignments totaled about $7 billion, over $6 billion of which went to the Department of Defense (DOD) and the Army Corps of Engineers; and FEMA grants to affected states totaled about $1 billion. In addition, some departments and agencies, including DOD, received direct appropriations for Hurricane Katrina activities. On September 24, 2005, Hurricane Rita brought further destruction to the Gulf Coast states of

Louisiana and Texas. This further compounded FEMA's already overburdened resources and infrastructure. Some estimate that the total federal response and recovery cost could reach $200 billion and more.

Based on our work related to prior emergency response efforts, we have raised concerns regarding weaknesses in FEMA information systems, the flood map modernization program, contract management, grants management, and the individual assistance program. When one considers that FEMA's programs are largely administered through grants and contracts, the circumstances created by Hurricanes Katrina and Rita provides an unprecedented opportunity for fraud, waste, and abuse.

While DHS is taking several steps to manage and control spending under Katrina, the sheer size of the response and recovery efforts will create an unprecedented need for oversight. We are overseeing the funds being spent directly by DHS components, and the OIGs of 12 other departments and agencies are overseeing their respective agencies' expenditures related to Katrina, which account for about 99 percent of the funds obligated to date for FEMA disaster response and recovery efforts. During the current response phase, the primary focus of the OIGs is on contracts, particularly those awarded with no or limited competition. In addition, we are conducting an evaluation to determine the overall adequacy of DHS' emergency management program for major natural disasters, i.e., how well FEMA carried out its disaster management responsibilities in response to Hurricanes Katrina and Rita.

Further, FEMA could benefit from improving the information technology systems it uses to both mitigate risk and respond to emergency incidents. For example, floods are among the most frequent and costly of all natural disasters and have great impact in terms of economic and human losses each year. FEMA has embarked on a six-year, $1.475 billion flood map modernization program to digitize flood maps used to identify flood zones and determine insurance requirements. The current maps are paper-based, outdated, inaccurate, and inadequate. Although FEMA is making progress in the program, its Multi-Year Flood Hazard Plan does not effectively address user and funding needs, and current policies, agreements, and information sharing mechanisms do not effectively support coordination and cooperation among mapping stakeholders.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components in 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. Further, in 2005, the Secretary initiated an internal top-to-bottom review of the Department, referred to as the Second Stage Review (2SR). The review resulted in changes to DHS organization structure. Those changes resulted in a DHS that was re-focused on risk and consequence management and further involved with its partners in other Federal agencies, state and local governments, and private sector organizations. However, much remains to be done.

For example, we reviewed and reported on a proposal to merge the Customs and Border Protection and Immigration and Customs Enforcement components within DHS. Our report, which will be issued shortly, identifies a number of significant concerns that need to be addressed, with or without a merger. In addition, as reported herein and in previous Management Challenges reports, we continue to have concerns about the Department's "dual accountability" structure for managing its business functions, particularly as related to the Chief Information Officer, Chief Financial Officer, and Chief Procurement Officer.

CONTRACT MANAGEMENT

DHS procured approximately $9.8 billion in goods and services during FY 2004 through the award of contracts, modifications, delivery orders, interagency agreements, and purchase card transactions. During the course of FY 2005 exclusive of Hurricane Katrina procurement actions, we identified a number of issues related to the challenge of building an effective contract and acquisition management infrastructure for this level of procurement activity. Those issues included the following:

- DHS needs to ensure adherence to required standards of conduct, i.e., the avoidance of improper business practices and conflicts of interest. While DHS' close relationship with the private sector may yield benefits for DHS, it also increases the potential for conflicts of interest. As noted above, we will be reviewing all Katrina related contracts awarded without competition.

- While some DHS organizational components have reported establishing program management processes within their components, currently no DHS organization is responsible for establishing Department-wide policies and procedures for program management operations. This function is critical, given the numerous, complex, mission-critical programs underway that are managed by DHS components. In May 2004, DHS instituted a program management certification process which requires increasing levels of program management certification (Levels I – III) based on varying levels of training and experience. However, some DHS organizational components still report a shortage of certified program managers to manage the Department's 110 major programs.

- DHS needs to institute several improvements to their Investment Review Board (IRB) process. For example, the DHS IRB process lacks detailed Departmental reviews, which provide decision makers with advice from functional experts, such as operational test evaluators and independent cost estimators. Also, the DHS IRB process emphasizes approval and scoring of a specific program plan, rather than selection from various alternatives.

- DHS has substantial staffing disparities in its procurement offices as the amount of awards per DHS procurement staff person ranges from a low of about $3 million up to $30 million per DHS procurement organization. In addition, some DHS procurement offices may be significantly understaffed, based on two separate studies sponsored by the Office of the Chief Procurement Officer (OCPO).

- DHS needs to establish an effective, independent oversight program. Currently there is no DHS management directive addressing OCPO oversight of DHS procurements. As a result, OCPO has limited authority to ensure compliance with DHS procurement policies and procedures. Establishing effective OCPO oversight could help DHS ensure adherence to standards of conduct, improve agency operations and ensure compliance with agency policies and procedures.

- Finally, several DHS components 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 $3.3 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost $19-24 billion and will take twenty to twenty five years 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. DHS OIG will be reviewing these major procurements on an ongoing basis.

GRANTS MANAGEMENT

DHS manages a variety of disaster and non-disaster grant programs. Disaster grant awards will be substantially more than usual with the over $60 billion appropriated in late FY 2005 for disaster response and recovery efforts related to Hurricane Katrina. Also in FY 2005, DHS expected to award approximately $4.6 billion of non-disaster grants.

We are 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. We will continue its audits of state and local governments' management of first responder grant funds and the Department's disaster relief programs, with special emphasis on Hurricane Katrina disaster response and recovery grant spending.

DHS needs to ensure that, to the maximum extent possible, homeland security assistance goes to those areas that represent the highest risks or vulnerabilities. For example, in our report on the DHS Port Security Grant program, the we reported that DHS grant making for this sector of national infrastructure was not well coordinated with the Information Analysis and Infrastructure Protection Directorate's (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 did 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 noted that the Office of State and Local Government Coordination and Preparedness (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, and that in FY 2005, SLGCP would involve IAIP's Office of Infrastructure Protection appropriately in the Port Security Grant Program. Department officials also said that in FY 2005, SLGCP plans to increase staff to allow for site visits and improved oversight of grant-funded projects.

FINANCIAL MANAGEMENT

DHS continues to face significant financial reporting problems, as evidenced by the FY 2004 and projected FY 2005 disclaimer of opinion on its consolidated financial statements. As of this date, we expect that continuing financial reporting deficiencies at ICE and Coast Guard will be the primary reasons for a FY 2005 disclaimer.

In FY 2005, ICE continues to struggle with financial management and reporting problems previously reported. In FY 2004, the financial statement auditors reported that ICE had fallen seriously behind in basic accounting functions, such as account reconciliations, analysis of material abnormal balances, and proper budgetary accounting. They reported that weaknesses in controls might have allowed ICE to violate the Anti-Deficiency Act or prevented management from knowing if they were in violation; however the auditors were unable to complete their procedures because ICE had not adequately maintained its accounting records. With respect to Coast Guard, we expect that issues related to its military pension liability; property, plant, and equipment; and operating materials and supplies will also contribute to a disclaimer of opinion.

DHS Financial Accountability Act

Under the DHS Financial Accountability Act, DHS must undergo an audit of internal controls over financial reporting beginning in FY 2006. To "pass" such an audit, DHS and its bureaus will have to document its identification, evaluation, and testing of relevant financial controls and implement corrective actions. DHS has taken several positive steps, including the formation of a working committee to address the requirements of the law. Notwithstanding DHS' commitment to fully comply with the law, this is a significant task and will require a sustained effort not only by the Office of the CFO, but by all managers throughout the Department. We will audit the Department's FY 2006 internal control attestation during our audit of the Department's FY 2006 financial statements.

HUMAN CAPITAL MANAGEMENT

The Homeland Security Act gave DHS special authorization to design a human capital management system that fits its unique missions. In June 2004, the Department awarded a contract for services related to the development and implementation of its new human capital management system, MAXHR, and in January 2005, the Department announced its final MAXHR regulations.

Although the Department intended to implement the new personnel system in the summer of 2005, district court decisions in July, August, and October enjoined the Department from implementing significant portions of MAXHR. Whether the Department appeals or proposes further modifications to the program, significant implementation delays are certain. Those delays will impact the cost of implementation, the current development and implementation contract, and the ability to properly and effectively manage its workforce.

We are coordinating with the Government Accountability Office to closely monitor DHS' efforts to create and implement its new human capital management system.

INTEGRATION OF INFORMATION SYSTEMS

Creating a single infrastructure for effective communications and information exchange at various classification levels within the Department remains a major management challenge for DHS. To meet this challenge, the Chief Information Officer (CIO) has outlined an Information Technology Infrastructure Transformation Program to create a secure, sensitive but unclassified network and a common email system for sharing across the Department. The program includes consolidating data centers, as a means of reducing costs and increasing reliability and survivability of the computing environment. Further, the program discusses plans for transforming helpdesk and other related support services. In September 2005, the Transformation Program was under review by the Department's senior leadership.

However, the DHS CIO is not well positioned to accomplish these IT integration 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. Although steps recently have been taken to formalize reporting relationships between the DHS CIO and the CIOs of major component organizations, the CIO still does not have sufficient staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support Departmental units. While the CIO currently participates as an integral member at each level of the investment review process, 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, including its intelligence systems, which address the risks and vulnerabilities facing DHS' IT systems.

As we reported in September 2005, based upon its annual FISMA evaluation (excluding its intelligence systems), DHS achieved two significant milestones that will help the Department move toward managing a successful information security program. First, DHS completed a comprehensive inventory of its major applications and general support systems for all DHS' components. Second, DHS implemented a Department-wide certification and accreditation (C&A) tool that incorporates the guidance required to adequately complete a C&A for all systems. The completion of these two tasks eliminated two factors that significantly held the Department back in achieving some success in establishing its security program in the last two years.

As we reported in our FY 2004 FISMA evaluation, and despite several major improvements in DHS' information security program, DHS' components have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices. For example, not all DHS systems have not been certified and accredited. The CIO has developed a detailed remediation plan to accredit all systems by September 2006. In addition, not all components' information security weaknesses are included in their Plan of Action and Milestones nor is the data in the enterprise management tool complete and current. To address this issue, the CIO will identify ways to improve the review process and increase accountability at the components. The CIO has also made numerous upgrades to its management tool, to improve the accuracy and completeness of the data.

The Department is also tasked to protect its national security systems. We reported in January 2005 that DHS needed to take steps to provide adequate security for the information and information systems that support its classified operations and assets. DHS must also ensure the confidentiality, integrity, and availability of vital classified information. DHS concurred with our recommendations.

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, DHS must identify and 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 75,000 national assets. However, the process the DHS 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 IAIP provided guidance for the collection of data, the data it received was often inconsistent. We are evaluating the effectiveness and efficiency of the processes that DHS 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 controlling the borders of the United States. This mission is shared by a number of agencies within the Department.

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 agency 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. Additionally, CBP and ICE have employees assigned outside the United States to protect the sovereignty of our borders.

Other DHS components share border security responsibilities. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is responsible for developing and fielding 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, the U.S. Citizenship and Immigration Services (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, including improved controls over the Visa Waiver Program and lost and stolen passports; and, reducing the immigration benefit application backlog.

For example, CBP needs to fuse the intelligence gathered with intelligence requirements to accomplish its priority mission. The CBP mission of preventing terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel is critical. Knowing the difference between legitimate trade and travel and terrorists is a challenge that timely intelligence often solves threat to our national security. The ability of CBP to gather and distribute intelligence information to field personnel has a direct effect on security at our borders. Border security also depends on information about terrorists kept on various watch lists. The watch lists are managed by several Federal agencies. Those agencies and DHS need to coordinate access to the lists to ensure valuable information flows through CBP to field personnel on the line.

Control over the northern border is another challenge. The external challenges to CBP's mission of managing, securing, and controlling our northern border include 128 ports of entry, thousands of miles of difficult terrain, large expanses of private property, and numerous lakes. The primary internal challenge to CBP is to ensure adequate resources are available. Resources on the northern border now include aircraft, vehicles, facilities, and officers, agents and specialists.

CBP must have sufficient number and type of personnel, equipment, and border infrastructure to achieve their mission on the northern, Canadian, border.

A further challenge for DHS are the difficulties CBP and ICE continue to experience coordinating and integrating their respective operations. More than two years after their creation, CBP and ICE have not come together to form a seamless border enforcement program. Their operations have significant interdependencies that have created conflict between CBP and ICE. Jurisdictional, operational, and communication gaps exist between the two organizations that must be addressed by DHS leadership.

We are continuing to maintain an aggressive audit and inspection program for the Department's border security initiatives to ensure that they are being carried out in an economical, efficient, and effective manner.

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. Our 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 and 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, improving management and supervision of screener activities, and testing new technologies.

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 alone does not ensure effective security. For example, TSA has not installed explosives detection technologies at the checkpoint to screen for explosives on the body. As noted above, TSA is in the process of testing several technologies that include backscatter x-ray, explosives trace portals, and document scanner machines to address concerns regarding detection of explosives on individuals. TSA is currently piloting these technologies at 16 commercial airports to assess the operational effectiveness of the technologies.

We are 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.

For example, there is growing concern that the resources being devoted by the Coast Guard to its Deepwater Program is reducing its ability to maintain and re-capitalize shore side infrastructure critical to its legacy and homeland security missions. The Coast Guard occupies more than 21,000 buildings and structures totaling more than 33 million square feet of building space. The estimated replacement value for these shore side assets is $7.5 billion. Based on this value, and recent and projected shore infrastructure acquisition, construction, and improvement (AC&I) funding levels, Coast Guard's recapitalization rate[1] hovers around 200 years. This is in sharp contrast to the Department of Defense's target recapitalization rate for its facilities of 67 years.

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. TSA requested $5.6 billion to facilitate its operations in FY06. However, only $32 million (less than 1 percent) of this request is earmarked for surface transportation security.

TRADE OPERATIONS AND SECURITY

Trade Operations and Security is primarily the responsibility of CBP. The Coast Guard and ICE also play important roles in support of this area. In a typical year CBP processes millions of sea containers; semi-tractor trailers; rail cars; millions of tons of bulk cargo; and liquids; such as chemicals, crude oil, and petroleum products. They also process or review all of the personnel associated with moving this cargo across our borders or to our seaports. CBP has the counterbalancing mission of facilitating the legitimate trade so vital to our country and at the

[1] Recapitalization rate is the number of years required to regenerate a physical plant – either through replacement or major renovation – at a given level of investment in order to keep the facility modern and relevant in an environment of changing standards and missions.

same time enforcing the laws associated with trade or border controls. CBP has the challenge of interdicting smuggling and stopping other illegal activities that benefit terrorists and their supporters.

Working with the trade, foreign allies, other DHS components, and other Federal, state and local agencies and organizations, CBP is intent on preventing legitimate commercial cargo from being used by smugglers and terrorists to introduce weapons of mass effect or other contraband into the U.S. CBP has implemented a number of initiatives to accomplish this objective such as the Container Security Initiative (CSI), and Customs-Trade Partnership Against Terrorism (C-TPAT). CSI works with foreign allies and partners to screen and examine containerized cargo at overseas port before it is loaded on ships bound for the U.S. The initiative calls for the increased use of non-intrusive technology to inspect this cargo both overseas and at U.S. ports. Within C-TPAT, CBP works with the trade to develop and implement processes and systems to help secure the supply chain. CBP uses targeting systems to assist in identifying the cargo that represents the highest risk, so that the use of precious and limited resources can be focused on this cargo. Other initiatives include developing a “smart” container that will provide extra protection or warning of tampering or intrusion. In support of CBP’s overall trade mission, they are undertaking an extensive and long-term effort to develop a new automated system (ACE) to replace older, less effective and capable trade processing systems. This effort is not scheduled to be fully competed until 2011, and will cost more than $3.3 billion dollars.

We issued a report regarding the Automated Targeting System (ATS) used to help identify high-risk cargo, and other aspects of the environment in which it is used. In this report, we made several observations about the trade supply chain and its vulnerabilities. We concluded that improvements could be made with regard to the data to which ATS targeting rules are applied, that examination results should be used more systematically in developing targeting rules, and that physical controls over containers selected for examination can be improved. As this review is legislatively mandated, we are currently reviewing other aspects of the ATS and its operational environment.

MANAGEMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REPORT ON MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

The following provides specific responses to those issues raised by the Inspector General's (IG) statement on the top management challenges facing the Department.

Disaster Response and Recovery

As highlighted in the IG Statement, the Department recognizes the need for oversight of spending on Katrina recovery efforts. The Department has taken numerous actions to address this issue. In addition to the IG teams now reviewing Katrina and Rita contracts, the Department is establishing a Katrina recovery contracting office to provide a dedicated procurement staff to oversee Katrina recovery contracting work and has formed a fraud, waste and abuse taskforce to ensure the proper financial controls are in place to manage the recovery effort. The Department has brought in outside expertise to conduct tests of FEMA's internal controls and to assess what organizational, staffing and business process changes are necessary for FEMA's financial management organizations to manage the supplemental funding. Dozens of detailees from Department Component CFO organizations have been assigned to FEMA to assist in budget and financial management of the response and recovery work. Secretary Chertoff has communicated to Congress that the Department will ensure that FEMA has mature, solid contracting and procurement systems in place before a disaster – and that those systems include a special focus on procurement integrity.

The Department is taking action to address the IG concern to improve FEMA information technology (IT) systems. During the Katrina response, our efforts were significantly hampered by a lack of information from the ground. With communication systems damaged and state and local assets compromised by the subsequent flooding, our ability to obtain precise reporting was significantly impaired. The sheer force of Hurricane Katrina disabled many of the communications systems that state and local authorities and first responders rely upon to communicate with each other and with FEMA. This was not an issue of interoperability, but of basic operability resulting from wind, flooding, loss of power, and other damage to infrastructure. We are ensuring sufficient communications capabilities are in place in the future and able to function during the worst phases of a hurricane or incident. Future communications must also ensure FEMA has its own increased communications capability so we do not face a similar situation. While satellite phones are helpful, they are not a panacea. We are looking at ways to adapt military and advanced private sector communication technology for emergency use – to help state and local first responders as well as FEMA support personnel.

We are also working to improve other FEMA IT systems related to the business processes for registering people for assistance, and getting them the benefits they need. The Department is evaluating FEMA's disaster registration processes and databases to make sure we have a high degree of confidence in those systems. We want to have the flexibility to use this information to provide a level of granular detail that enables us to make informed decisions about where to focus our attention and resources, and how to better assist our state and local partners.

In response to the OIG's concern regarding the Multi-Year Flood Hazard Plan, FEMA's 5-year budget and schedule plan for flood hazard data development was issued November 2004 and updated June 2005.

This plan reflects funding received and anticipated from the President and Congress. FEMA recognizes that this level of funding does not meet all of the needs of our State and local mapping partners; however, it is important to note that FEMA's role in flood map modernization focuses on essential flood mapping requirements and must be complemented by others. A business planning and standards improvement process with stakeholders is in place to facilitate collaboration and coordination on plan improvements. FEMA is currently evaluating the level of funding required for flood map maintenance. A Partnership Building Plan was issued in March 2005 to develop and implement better strategies for partnering with state and local entities with varying levels of capabilities and resources. In addition, FEMA issued a formal policy on geospatial data coordination in August 2005, and established a geospatial data coordination and standardization management team to support the implementation of the policy in cooperation with stakeholders.

Consolidating the Department's Components

Proposed changes to the Department of Homeland Security's structure and organization as a result of the Second Stage Review are designed to improve our capabilities to protect and safeguard this nation. One critical need within the Department is to have the capacity to think through broad and overarching issues with a Department-wide perspective, rather than just through the lenses of one particular component. By integrating and coordinating areas of intelligence, policy, operations and preparedness efforts, this Department will be in a stronger position to respond actively to present and future threats with appropriate actions and policies.

In regards to consolidating the Department's components, the IG raised the issue regarding the proposal to merge CBP and ICE. Based on the Second State Review of the entire Department, the Secretary determined that ICE and CBP would not be merged. To address the coordination issues involving intelligence, operations, and policy, the Secretary determined that a reorganization of the Department would best address these coordination issues for the entire Department, including ICE and CBP. New policy, operations, and intelligence directorates are being established to facilitate coordination between all of the Department's components in the areas of policy, operations, and intelligence.

Another issue raised by the IG in this arena was the effectiveness of the dual accountability structure for business operations. The Department has implemented the dual accountability structure during fiscal year 2005, and the system has assisted in the integration and streamlining of support service functions. Creating functional excellence required every executive, manager, and employee in the Department to create an environment that rewards collaboration, promotes best practices, and shares accountability for the performance of the management support systems that enable the Department to fulfill its missions. The concept of dual accountability mandates that both components and key departmental functional experts are responsible for organizational excellences. The department functional experts are held accountable for designing systems to optimize service functions, setting the standards for function performance, creating the department-wide policies and processes, providing the automated solutions to yield greater efficiencies, and nurturing the development and success of centers of excellence. Components are likewise accountable to support these progressive business functions as s key pert of their commitment to mission accomplishment.

In all efforts of this magnitude, when so much is to be gained, the integration and alignment of each function requires strong communication, respect for both individuals and processes, and a shared resolve to finds solutions that benefit both mission accomplishment and functional excellence. Leadership across the Department is challenging traditional approaches, communicating, and executing as a team to design and execute support functions that will constitute progressive 21st century excellence in governance.

Contract Management

While the IG report highlights some ongoing challenges in the contract management arena, there have been improvements since last year in the Department's contract management system. For instance, clear lines of responsibility have been established in this arena. The Undersecretary of Management

(USM) is responsible for establishing department-wide policies and procedures for program management operations. Within USM, the CPO has responsibility for the acquisition workforce, acquisition policy, and oversight. The CFO's Program Analysis and Evaluation (PA&E) office is responsible for coordinating reviews for the Investment Review Board and Joint Requirements Council (JRC), which provide Department oversight of major acquisitions.

The Department recognizes that ensuring the necessary numbers of certified program management staff are present is a multi year issue, and is actively working to increase the number of certified program management staff in the Department. The Department currently has an agreement with the Defense Acquisition University for program management training. The Department is instituting improvements to the IRB process, the most notable being implementing an integrated review process to provide decision makers with advice from functional experts (within the CFO, CIO, CPO, CAO, S&T, Policy, General Law & Privacy). The department is also developing procedures for independent verification and validation (IV&V) of major investments, addressing another IG concern. As part of the IRB governance process, additional emphasis is placed on assuring that a program management office is in place on Level I and II initiatives.

The Department concurs with the IG that several high visibility investments in the Department (ACE, US-VISIT, Deepwater) require close management. These investments are reviewed quarterly when they submit their status reports that are required by Congress, along with an intensive review that occurs with submittal for approval of their annual expenditures plans. The Department is working to implement a quarterly reporting process for all major investments that will gauge project management efforts in terms of adherence to cost, schedule, and performance.

To address the staffing disparities in procurement offices, the CPO established target staffing levels and communicated this to Department components in writing. The CPO provided input to the CFO for the fiscal year 2007 to fiscal year 2011 budget to support the target staffing levels.

Grants Management

State and Local Government Coordination and Preparedness (SLGCP) has taken a number of steps to address the grants management challenges identified in the IG. First is the establishment of SLGCP's internal grant financial management office, the Office of Grant Operations (OGO). Effective October 1, 2005, OGO assumed responsibility for all pre- and post-award grant financial management activities for the SLGCP programs currently serviced by its legacy Department of Justice organization. The OGO staff has defined its financial monitoring parameters and objectives and is finalizing its fiscal year 2006 monitoring plan and site visit/desk review guidelines. The goal is to ensure that adequate financial monitoring is performed on SLGCP's expanding portfolio of grants. During the month of October 2005, OGO will begin fulfilling monitoring objectives by performing site visits in tandem with program managers from SLGCP's Preparedness Programs Division (PPD). Another step taken to address these management challenges is the establishment of the Transportation Infrastructure Security Division (TISD) within PPD. This Division is staffed by transportation subject matter experts, and was created specifically to manage the transportation-related grant programs inherited from the Transportation Security Administration (TSA).

The second major accomplishment is the use of risk criteria in making grant allocation decisions. Specifically, SLGCP, in coordination with IAIP and the Coast Guard, refined the fiscal year 2005 Port Security Grant Program to make the allocation of funds more risk-based. As part of this process, a risk-based formula was used to limit eligibility to the nation's sixty-six (66) most at-risk ports. In addition, national port security priorities were identified for the program, and the application review process was sharpened to focus on these national priorities, as well as local port security factors like alignment with the port's Area Maritime Security Plan. Based on these program enhancements, the Department's IG concluded that SLGCP had sufficiently responded to the recommendations contained in IG Report 05-10, Review of the Port Security Grant Program, and closed all of the recommendations contained in this report in July, 2005.

At the outset, the Department acknowledges that although we have substantial resources to provide security, these resources are not unlimited. Therefore, we as a nation must make tough choices about how to invest finite human and financial capital to attain the optimal state of preparedness. In making the tough choices on where and how to invest in security, the Department will focus preparedness on objective measures of risk and performance. This risk analysis is based on these three variables: (1) threat; (2) vulnerability; and (3) consequences. These variables are not equal – for example, some infrastructure is quite vulnerable, but the consequences of attack are relatively small; other infrastructure may be much less vulnerable, but the consequences of a successful attack are very high, even catastrophic.

The Department will concentrate first and most relentlessly on addressing threats that pose catastrophic consequences. Some of the tools needed to prevent, respond and recover from such awful scenarios are already in place; but others need significant improvement. The first step in enhancing national preparedness is establishing a preparedness baseline that measures the effectiveness of our planning for preventing, protecting against, and responding to terrorist acts or disasters. A Department review team has, therefore, constructed the model for an analytic matrix that will set that baseline. The matrix will allow us to analyze possible threats and will map the current state of prevention, protection and response planning with regard to each. This matrix will be a critical tool enabling us to identify and remedy current gaps in preparedness.

Bringing greater planning discipline to each of these risk scenarios ensures we secure the highest risk areas, especially in executing our preparedness mission. And simple common sense counsels that we begin by concentrating on events with the greatest potential consequences. That is why the Department's *National Preparedness Goal* -- and additional, risk-based planning -- will form our standard in allocating future Department grants to our state and local partners so that we build the right capabilities in the right places at the right level. Federal money will be distributed using the risk-based approach that we will apply to all preparedness activities.

Financial Management

The Department is committed to world-class financial management. The Department continues to proactively monitor the management and oversight of financial management improvements for ICE and Coast Guard as well as other Department components whose deficiencies in internal control compromise the integrity of financial reporting in the department. All Department components have corrective action plans to fix existing material weaknesses identified in the audit to achieve an unqualified audit opinion on the consolidated financial statements. The Department's CFO has instituted a Three Year Vision for Financial Reporting to position the Department for an unqualified opinion on the fiscal year 2007 financial statements. The Department's CFO's Office (OCFO) continues to meet regularly with all the Department components, including Coast Guard and ICE to assess progress against both the correct action plan and CFO's Vision, and to discuss and resolve problem areas.

The OCFO is continuing its efforts to functionally integrate the financial management line of business activities at the Department. The OCFO has already realized progress toward the vision of a unified financial management system for the Department by reducing and consolidating the number of disparate budget, finance, and accounting processes, providers, and systems. Since the Department's inception, OCFO has reduced the number of accounting providers from nineteen to eight. The OCFO is continuing to enhance its guidance to and oversight of Components and is making significant progress in establishing Department-wide standard operating procedures and policies, particularly in the areas of budget execution, financial management, and financial reporting. We will continue to work with the IG as we proceed to improve our financial management practices.

DHS Financial Accountability Act

Fiscal year 2005 proved to be a watershed year for internal controls at the Department of Homeland Security. Shortly after passage of the DHS Financial Accountability Act, the Department developed a strategy and vision for implementation. Most notably, the Department established an Internal Control Committee (ICC) responsible for improving internal controls. ICC membership includes a Senior Management Council, ICC Board, and Senior Assessment Team. The Senior Management Council is comprised of the Department's Under Secretary for Management, CAO, CFO, CHCO, CIO, and CPO. Their function entails overall management accountability, monitoring of corrective action plans, and ICC sponsorship. The ICC Board seeks to integrate and coordinate internal control assessments with other internal control-related activities and includes representatives from all Department lines of business to address crosscutting internal control challenges. Finally, the Senior Assessment Team comprised of senior level financial managers carries out and directs Component level internal control assessments. Over the past year the ICC has:

- Published our landmark implementation guide, which is specifically tailored to support an attestation on internal control over financial reporting as required by the DHS Financial Accountability Act.
- Developed a comprehensive integrated framework for the Federal Financial Managers' Financial Integrity Act and have taken significant steps to prepare for implementing the recent revisions to OMB Circular A-123, Management's Responsibility for Internal Control, effective in fiscal year 2006.
- Implemented the GAO Internal Control Management and Evaluation Tool across the Department to facilitate the development of internal control activities in accordance with GAO's Standards for Internal Control in the Federal Government.
- Initiated a seven-step plan to prepare for the fiscal year 2006 audit of internal controls over financial reporting.
- Completed a comprehensive internal control assessment of the consolidated financial reporting process within the OCFO. In addition, the Coast Guard, one of our largest Components, has initiated process level documentation pilots.
- Developed corrective action plans for all material weaknesses and reportable conditions and a Management Directive and Process Guide to ensure these corrective action plans demonstrate results.

Human Capital Management

While the District court decisions have enjoined the Department from implementing certain portions of MAX^{HR}, the classification, pay and performance management provisions of the new human resources management program are moving forward. Deployment of the new performance management system is being implemented for covered employees, including managers, supervisors, non bargaining unit employees, in Headquarters starting in October 2005, and will be expanded during fiscal year 2006 to other Department components, such as FLETC, Secret Service, USCG, FEMA and ICE. Significant design work will continue on the new pay system with planned implementation by January 2007 for phase 1 organizations, such as HQs, Secret Service, USCG, FEMA and FLETC. Emphasis on performance management training for all audiences, i.e., managers, supervisors, HR specialists, systems administrators, and all employees, will continue throughout fiscal year 2006. The Department also evaluated the impact on the fiscal year 2006 funding requirement and reduced the request accordingly. It is anticipated that the overall cost for full implementation will not increase.

Integration of Information Systems

CIO believes it is properly positioned and has the authority it needs to accomplish its mission. The CIO is the principal IT authority to the Secretary and Deputy Secretary, and it will continue to hold that leadership role within the Department. The CIO continues to work on the integration of its information systems. To that end, the Infrastructure Transformation Office (ITP) has been tasked with improving information sharing and interoperability, providing a reliable and scalable infrastructure, and managing costs efficiently. To effectively manage this transformation from over 20 individual, stand-alone IT infrastructures with minimal interconnectivity, to a single, cohesive IT infrastructure, the ITP is organized by the following project areas:

- **Network Services:** Establish an integrated enterprise network for the Department by streamlining and standardizing the network environment, minimizing the amount of redundant IT infrastructure, providing operational and security support, and developing a Department-wide network topology with centralized governance and standardized procedures.

- **Email Services**: Establish a common, SBU e-mail system for the Department and provide enterprise directory services.

- **Help Desk and Related Services:** Establish a centralized help desk capability to resolve issues such as network connectivity, data access, and email access.

- **Data Center Services:** Establish two data center facilities that will improve information availability by standardizing backup functionality, improve security by reducing the number of locations and consolidating network entry points, improve system reliability by employing enhanced environmentals, and improve the real-time availability of Department data.

- **Video Services:** Establish a standard, enterprise-wide video operations capability for the Department.

Security of Information Technology Infrastructure

The success of the Department's mission is absolutely dependent on our ability to protect sensitive information used in defending the homeland. While much of the Information Security Program is structured around compliance with FISMA, OMB and National Institute of Standards and Technology (NIST) standards and guidance, the Department's Information Security Program has also been designed to provide a secure and trusted computing environment based on sound, risk-management principles and program planning.

We agree that compliance on the part of the Department component organizations is paramount to the success of a Departmental information security plan. To this end, the Office of the CIO recently completed a comprehensive inventory of all information systems currently in use within the components, as well as in the headquarters organizations. This inventory followed a common methodology for determining appropriate security boundaries and will now serve as the baseline for systematically improving our systems security. This framework of common inventory definitions, coupled with recently deployed enterprise-wide security management tools and processes, will provide the common trust environment that is necessary for negotiating effective and appropriate rules-of-behavior across system boundaries, thereby facilitating information sharing.

Infrastructure Threat Assessment

The IG raised concern about the Department's ability to gather information for the National Asset Database (NADB). As of August 2005, the NADB contained nearly 100,000 assets with tens of thousands of other assets available for inclusion. It is important to note that the process of assessing threats against the assets, determining the vulnerability of an asset, and prioritizing the threat mitigation effort is inexorably tied to the data collection effort itself. Data collection is a challenge as Information Protection relies on a myriad of sources for data, and is without a preexisting legal or regulatory framework for data collection or prioritization of information. The Department has been successful in building the needed capabilities, and results are now beginning to emerge. While there is no precedent for collecting the extensive information that forms the NADB, IAIP is leading the way and has created a blueprint for collecting the information and conducting the analysis.

Border Security

We agree with the OIG's assessment that the Department faces several formidable challenges in securing the nation's borders. The Department is aggressively addressing these issues and the solutions will require dedicated management oversight. We have developed a comprehensive multi-year plan to secure America's borders and reduce illegal immigration, referred to as the Secure Border Initiative (SBI). To facilitate implementation of SBI, the Department is establishing a program office at the department level to coordinate and integrate policy, provide procurement oversight, and facilitate inter-agency participation for this border and interior enforcement initiative. This includes coordinating and integrating CBP and ICE efforts to form a more seamless border security program. Since resources are not infinite, this program will use a risk based approach to deploy personnel, technology and border infrastructure at both the northern and southern borders.

We will address all aspects of the border security problem across the board – deterrence, detection, response, apprehension, detention, and removal. We will address the challenges in each of these areas with an integrated mix of increased staffing, more robust interior enforcement, greater investment in detection technology and infrastructure, and enhanced coordination on federal, state, local, and international levels. The Department has already made improvements to secure our borders and enforce immigration laws since 9/11. The Department has over 11,000 Border Patrol agents along more than 6,000 miles of northern and southern border, an increase of 15% over 9/11 levels, and is currently adding 1,500 more Border Patrol Agents. An additional 18,000 officers are posted at our Ports of Entry (POE), and over 8,000 agents and officers working to apprehend criminals, absconders, and other individuals illegally in the United States. Despite our substantial progress, we still face a substantial problem. The ability of individuals to enter our country outside legal channels is a threat to our homeland security. Flagrant violation of our borders undercuts the rule of law, undermines our security, and imposes particular economic strains on our border communities.

SBI is designed to enable the Department to achieve operational control of both the northern and southern border within five years. Key elements of SBI include:

- More agents to patrol our borders, secure our ports of entry and enforce immigration laws.
- Expanded and more efficient detention and removal capabilities to eliminate "catch and release" once and for all.
- A comprehensive and systemic upgrading of the technology used in patrolling the border, including increased manned aerial assets, expanded use of UAVs, and next-generation detection technology.
- Increased investment in infrastructure improvements at the border – providing additional physical security to sharply reduce illegal border crossings.
- Greatly increased interior enforcement of our immigration laws – including more robust worksite enforcement.

In response to other Border Security concerns raised by the IG, US-VISIT continues to be a top priority for the Department. US-VISIT entry procedures are currently in place at 115 airports, 15 seaports and in the secondary inspection areas of the 50 busiest land ports of entry. US-VISIT exit procedures are operating at 12 airports and two seaports. Entry procedures will be deployed to the remaining land ports of entry by December 31, 2005.

Efforts to integrate the Department's Automated Biometric identification System (IDENT) system with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) fingerprint system are moving forward. DHS is implementing a plan to transition to 10-print finger print capture in collaboration with Commerce, State, Defense, Justice and State Departments. Immediate 10-print transition efforts will be focused on enrollment efforts, and an initial IDENT/IAFIS interoperability solution is planned within 6 months of this transition. The plan proposes to:

- Begin enrolling foreign nationals using 10-print, while conducting current background checks
- Push aggressive investment to drive biometric technology market to deliver scanning equipment capability
- Improve IDENT to improve accuracy and watch list matching
- Continue to support IDENT/IAFIS interoperability work

To strengthen document integrity, the Department is now requiring a digital photograph of the passport holder's face printed on the data page of the passport after extensive consultation with Congress and the Department of State. The Department imposed an October 26, 2006 deadline for the integrated circuit chip, or e-passport, capable of storing the biographic information from the data page, a digitized photograph, and other biometric information in travel documents. Valid passports issued before October 26, 2005, will still be accepted for travel under the auspices of the Visa Waiver Program (VWP), provided that the passports are machine-readable.

In addition to the digital photo and chip requirements, the Department is taking steps to strengthen document integrity by requiring VWP countries to commit to several measures concerning lost and stolen passports. Among them, the Department will require VWP countries to report all lost and stolen passports to INTERPOL and to the Department, and increase information sharing between VWP countries and the United States government on trends and analysis of lost and stolen passports.

In response to another issue raised by the IG, the Department is committed to reducing the backlog of immigration cases. The goal is to reduce the cycle time for all cases to six months or less. Significant productivity gains must be realized to meet the target of a six-month cycle time for all immigration benefit applications by the end of fiscal year 2006. As such, USCIS is reengineering business processes, increasing the use of information technology to achieve greater efficiencies, updating policies and procedures to increase uniformity of decision making within the adjudication process, managing against milestones, and working cooperatively with stakeholders to identify other means of improvement. USCIS also will intensify its anti-fraud efforts, enhance its quality program, and modernize its information technology systems that will be the backbone of reengineered business processes. The combination of these efforts will ensure we reduce the backlog.

Transportation Security

Airport Screeners

A Department IG undercover audit of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not introduced into the sterile areas of airports and that explosives, 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, improving management and supervision of screener activities, and testing new technologies.

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). TSA has also deployed technologies, including explosives trace detection (ETD) devices, to detect potential explosives in carry-on baggage. However, deployment of the equipment does not ensure effective security; resolution of technology alarms is a key element to effective security. In the area of checkpoint technology, TSA has installed table top explosives trace detection technologies at the checkpoint to provide some capabilities when screening suspect carry-on items, electronic items, shoes, etc. To increase and automate these capabilities at the checkpoint, TSA has tested several technologies that include explosives detection trace portals and explosives detection document scanners to address detection of explosives on individuals. Based on the results of these pilots, TSA is now deploying the portals to the nation's largest airports. The document scanner that was piloted, while effective, was not determined to be efficient, therefore; TSA has reengaged technology manufacturers to develop an automated document scanner that will provide efficiencies and effectiveness. TSA is also planning to pilot other emerging technologies in fiscal year 2006, to include an automated explosives detection system for carry-on baggage to replace standard x-ray technology, and whole body imaging technology (x-ray backscatter) for screening persons for both weapons and explosives.

Maritime Security

The United States Coast Guard has been diligent in its mission to provide the nation with maritime security. They are meeting their challenges through a myriad of initiatives including:

- On-going delivery of the Integrated Deepwater System (IDS) including: construction of the first two Maritime Security Cutters-Large to be delivered in fiscal years 2007 and 2008, initial design of the Maritime Patrol Coastal (WPC) and the Maritime

- Security Cutter-Medium; production of the first two Maritime Patrol Aircraft and two Vertical Unmanned Aerial Vehicle (VUAV) to be delivered in fiscal year 2006; continued development of a Common Operating Picture at shore-based Command Centers, an Integrated Logistics Support System and legacy sustainment/enhancement projects for all major cutters and aircraft, including continued re-engineering of the HH-65 short-range helicopter fleet.

- Implementation of the Maritime Transportation Security Act (MTSA) of 2002: In fiscal year 2005 the USCG added 500 personnel to develop, review, and approve approximately 9,000 domestic vessel security plans and 3,200 domestic facility plans; develop 48 Area Maritime Security Plans and Committees; perform 55 domestic Port Security Assessments; develop a national Maritime Transportation Security Plan, verify security plan implementation on 8,100 foreign vessels and continue conducting foreign port security assessments on 100+ countries conducting direct trade with U.S.

- Continuation of the Great Lakes Icebreaker (GLIB) project, which will reach full operating capability in fiscal year 2006.

- Continuation of the Rescue 21 project, recapitalizing the USCG's coastal zone communications network, to ensure completion by the end of fiscal year 2007.

- Adding nearly 100 new personnel to support planning and coordination of all USCG mission at Command Centers.

- Continue implementation of the nationwide Automatic Identification System (AIS), significantly enhancing Maritime Domain Awareness (MDA) and improving the USCG's ability to detect maritime security threats farther from the nation's ports.

- Procurement of new Response Boats: Continue recapitalization of the USCG's obsolete, non-standard utility boats and increase the USCG's presence in critical ports and coastal zones.

- Commence Airborne Use of Force (AUF) implementation on the USCG's entire fleet of helicopters by arming existing helicopters at various Air Stations. AUF capability will improve performance of all homeland security missions, including enhanced protection of U.S. ports.

- Continue C-130J Maritime Patrol Aircraft (MPA) missionization. This project will provide additional MPA resources, enhancing MDA and resulting in increased ability to detect, identify, and monitor maritime security threats such as illegal drug traffickers. Armed with MPA surveillance information, USCG operational commanders can optimize use of surface assets and rotary wing aircraft through targeted interdiction of known threats.

- Added 55 billets for enhancing intelligence collection and oversight as a member of the national Intelligence Community. The staff will support critical maritime intelligence support nodes, the USCG Central Adjudication Facility (CGCAF) at the Security Center in Chesapeake, Va., and program management at the strategic-level.

Other Transportation Modes

In addition to aviation security, TSA is tasked with managing the security risk to the U.S. surface transportation systems while ensuring the freedom of movement of people and commerce. These systems include nine billion passenger trips per year on the nation's mass transit systems, over 161,000 miles of interstate and national highways and their integrated bridges and tunnels, and nearly 800,000 shipments of hazardous materials (95 percent by truck). For these systems, TSA will address these security responsibilities in partnership with other components of the Department as well as the DOT and other Departments.

TSA has provided the top 10 mass transit and passenger rail agencies with TSA-certified explosives detection canine teams to aid in the identification of explosives materials within the mass transit/rail transportation system. In addition, TSA has hired and deployed 100 surface transportation (rail) inspectors to enhance the level of national transportation security by leveraging private and public partnerships through a consistent national program of compliance reviews, audits, and enforcement actions pertaining to required standards and directives. TSA has implemented computer security and tools to ensure that risk and vulnerability assessments are performed leading to full certification and accreditation of major application and general support systems and to provide a Computer Security Incident Response Capability.

Trade Operations and Security

The Department has developed a multi-layered approach to ensure the safety and security of our trade operations, including several efforts focused on container and supply chain security, namely the Container Security Initiative (CSI), the Customs Trade Partnership Against Terrorism (C-TPAT), and the Automated Targeting System (ATS). In post-9/11 America, CSI is based on an idea that makes sense: extend our zone of security outward so that American borders are the last line of defense, not the first. Through CSI, maritime containers that pose a risk for terrorism are identified and examined at foreign ports before they are shipped to the United States. Early on, CSI focused on implementing the program at the top 20 foreign ports which ship approximately two thirds of the volume of containers to the U.S. Governments from these 20 foreign ports have already agreed to implement CSI. As CSI has evolved, CBP hopes to expand the program to additional ports based on volume, location and strategic concerns.

Strong support from countries on the European, Asian and African continents ensure that CSI will continue to expand to ports in those areas.

Since October 2004, CBP and the trade community have worked collaboratively to develop minimum security criteria for importers either already enrolled in the C-TPAT program, or wishing to join this voluntary supply chain security program. These new minimum security criteria help solidify membership expectations, and more clearly define and establish the baseline level of security measures which must be employed by member importers. These security criteria are effective as of March 25, 2005. A phased implementation schedule has been implemented and applies to all C-TPAT Importer members.
ATS is an aggressive, sophisticated targeting tool that enhances Customs ability to perform enforcement operations. ATS is a system that will assist Customs officers in identifying imports which pose a high risk of containing narcotics or other contraband. The system standardizes bill-of-lading, entry, and entry summary data received from the Automated Commercial System (ACS) and creates integrated records called "shipments". These shipments are then evaluated and scored by ATS, through the use of over 300 weighted rules derived from targeting methods used by experienced Customs personnel. The higher the score, the more the shipment warrants attention. The system allows inspectors to concentrate on higher-risk shipments for further screening and examination. It provides inspectional personnel with the ability to conduct quick data analysis of profile information accumulated on shippers, carriers and importers. ATS is operating in Newark, NJ, Laredo, TX, Seattle, WA, and the Port of Los Angeles/Long Beach, California. Future plans include the installation of ATS at all major seaports, airports, and land border ports of entry. It may also be expanded to outbound operations to target export cargo for anti-terrorism, currency smuggling, and other export violations.

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Executive Secretariat
Chief of Staff
General Counsel
Under Secretary, Management
Assistant Secretary, Public Affairs
Assistant Secretary for Policy
Assistant Secretary, Legislative Affairs
Chief Financial Officer
Chief Information Officer
Chief Security Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Program Examiner

Congress

Committee on Homeland Security and Governmental Affairs
United States Senate

Committee on Homeland Security
United States House of Representatives

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or email DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.