DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General
Washington, DC 20528

December 31, 2003

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

During its first nine months of existence, the Department of Homeland Security (DHS) has faced the challenge of effectuating the largest reorganization of the federal government in more than half a century, and creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack. 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) has identified the areas listed below as "major management challenges" facing the department. This list will be used in setting DHS OIG priorities for audits, inspections, and evaluations of DHS programs and operations. This is the second such assessment we have issued since the establishment of the department, and we will continue to issue these assessments on an annual basis.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Perhaps the biggest challenge facing DHS is integrating 22 separate components into a single, effective, efficient and economical department with about 180,000 employees. DHS has several integration efforts under way that OIG will monitor and assess on an ongoing basis. For example, according to DHS management, a total of over 350 different management processes, some of which were duplicative, have been reduced to 130. Similarly, the department has reduced from over 2500 in Fiscal Year (FY) 03 to roughly 600 the number of services that are provided under Memoranda of Understanding (MOUs) with non-DHS providers. The services, formerly supplied under these MOUs and now supplied by DHS, include payroll, mail, personnel security, and other critical services.

Further, one of the top priorities of the department was to integrate specific functions to enhance efficiencies and create greater accountability in one seamless border service. For the first time in the country's history, all agencies in the United States government with significant border responsibilities have been unified into one agency of our government.

DHS also reports that, using a "shared services" model, it has realigned over 6000 support services employee slots (both government and contractor) from the legacy U.S. Customs Service and the Immigration and Naturalization Service (INS) to support the 68,000 employees of the Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and Citizenship and Immigration Services (CIS) bureaus.

The department has deployed information technology (IT) systems to allow DHS employees to communicate internally and for the American public to communicate with the department, including headquarters network and email systems, intranet, and internet sites.

DHS has developed human resources (HR) policies and practices that enabled directorates and headquarters organizations to begin building their staffs. In addition, DHS assembled a design team, composed of DHS managers and employees, HR experts from DHS and the Office of Personnel Management (OPM), and representatives from the department's three largest unions, to study and prepare options for transforming the department's HR system and finalizing the policy for the new HR management system in alignment with the unique mission of the department.

The department has also established a Strategic Sourcing Group (SSG) to implement a DHS-wide approach to acquiring goods and services. The SSG has established commodity councils that are working to identify the department's needs for each commodity and to develop more efficient purchasing mechanisms to meet those needs. The total number of commodity councils established thus far is 17, covering such items as office supplies, copiers, weapons and ammunition, uniforms, and electricity. Also, DHS has established a Resources Management Transformation Office to oversee the development of an integrated financial management system for use department-wide.

To a great degree, however, the department is still a collection of separate components operating under a common organizational umbrella. Appropriate plans (including workforce plans), goals, objectives, and meaningful performance measures must be established as soon as possible to guide the integration process, track progress, and support effective planning and budget allocation across the full range of DHS' missions. Efforts to do so are under way. For example, DHS is implementing a ten-step process to create, validate, and institutionalize measures of effectiveness in critical performance areas. OIG will monitor this process as it proceeds.

CONTRACT MANAGEMENT

A major challenge for the department is integrating the procurement functions of its component organizations, some lacking important management controls. For example, during its first year of operation, the Transportation Security Administration (TSA) relied extensively on contractors to accomplish its mission, while providing little contract oversight. As a result, the cost of those initial contracts ballooned. TSA is in the process of devising policies and procedures that require adequate procurement planning, contract structure, and contract oversight.

Other components of the department have some large, complex, high-cost procurement programs under way that need to be closely managed. For example, CBP's Automated Commercial Environment project will cost $5 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost $17 billion and take two to three decades to complete. Further, in early 2004, the department will award a contract for the development of an automated 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. It is anticipated that this will be a multi-billion dollar program implemented over the next ten years. DHS OIG will be reviewing these major procurements on an ongoing basis. In addition, DHS recently developed a comprehensive list of department contracts as of March 1, 2003, which OIG is reviewing.

GRANTS MANAGEMENT

DHS manages a variety of grant programs that provide money for disaster preparedness and response and prevention. Significant shortcomings have been identified in many of these programs in the past, and the potential for overlap and duplicate funding has grown as the number of grant programs has grown. For example, DHS OIG's report on the Assistance to Firefighters Grant Program (OIG-ISP-01-03, September 2003) pointed out that many items authorized for purchase under the program are also authorized for purchase under the State Homeland Security Grant Program. In addition, preparedness grant programs are located in different DHS directorates. Having similar grant programs in separate organizations within DHS creates challenges related to inter-departmental coordination, performance accountability, and fiscal accountability. Furthermore, DHS program managers have yet to develop meaningful performance measures necessary to determine whether the grant programs have actually enhanced state and local capabilities to respond to terrorist attacks and natural disasters.

We are currently reviewing the delivery of Office for Domestic Preparedness first responder grants to states and local jurisdictions to identify problems in getting funds to first responders in a timely manner. In FY04, we will conduct audits of individual states' management of first responder grants and analyze the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. We will also continue our audits of the department's disaster relief programs.

FINANCIAL MANAGEMENT

Integration and Reporting

The most immediate financial management challenge for DHS has been the integration of the financial operations of its 22 components and the creation of its own central financial management processes. This process is ongoing. At the same time, the department must seek longer-term solutions to serious financial system problems inherited from legacy agencies. Finding the systems to correct these longstanding problems, but which also optimize DHS' financial operations, is a huge challenge. The Chief Financial Officer has established a working group to address this matter.

Although the department has many financial reporting requirements, one of the most notable will be its Performance and Accountability Report, which will include DHS' first set of audited financial statements. The mid-year creation of DHS with a full year transition period thereafter created special one-time circumstances that should, for the most part, not be

repeated in FY 2004. DHS will then be able to provide additional focus on its consolidation efforts and on improving its financial reporting processes.

Revenue Collection

Annually, CBP collects more that $22 billion in duties, excise taxes, fines, penalties and other revenue. With regard to one kind of such revenue, the Treasury OIG conducted a review of CBP's international mail operations and found that information on values from the mail declarations is often inaccurate and reliance on such information has resulted in CBP's losing revenue. The results of a CBP mail revenue survey for fiscal year 2001 showed that CBP loses an estimated $494 million per year based on examination of the contents of parcels.

Also, both ICE and CIS perform a key revenue generating role in collecting and accounting for the more than $2 billion in application fees from non-citizens seeking entry into the U.S. In fulfilling its mission, CIS processes millions of actions and requests that are documented in paper files. The systems that track these applications are non-integrated, and many are ad hoc. As a result, CIS has had to halt normal business operations for up to two weeks in past years in order to determine and report deferred revenue. Deferred revenue is a financial measure of pending applications and is material to DHS' accurate financial statements. The challenge for CIS is to move from paper based and non-integrated processes to an integrated case management system, which CIS is in the process of doing.

Further, CBP is responsible for collecting user fees from air passengers arriving in the U.S. The fees are designed to pay for the costs of inspection services provided by CBP, which now includes the 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 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 pay for the costs of providing civil aviation security services provided by screening personnel, federal air marshals, and equipment. OIG plans to conduct audit activity during FY04 that will address these issues.

HUMAN CAPITAL MANAGEMENT

The Homeland Security Act gave DHS special authorization to design a human capital management system that fits its unique missions. As noted above, 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 will be published as proposed regulations. 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.

BORDER SECURITY

CBP and ICE share responsibility for ensuring the security of the U.S. borders. CBP's focus is on security at and between the ports of entry along the border, and it is responsible for enforcing customs and immigration laws, with emphasis on the movement of goods and people. Employees from the former Customs Service, INS, APHIS, and the Border Patrol work together to accomplish this mission. ICE's focus is on enforcement of immigration and customs laws. The inspectors and agents place heavy reliance on various information systems and high technology equipment to secure the borders against terrorists, weapons of mass destruction, illicit narcotics, and other illegal activity. Prior to DHS' establishment, OIGs at both the Departments of Justice (DOJ) and Treasury, as well as the General Accounting Office, identified numerous deficiencies in the systems used to track aliens, and in the deployment, use, and operational effectiveness of the equipment used to meet the border security mission. To a great extent, these challenges remain.

Specific challenges include the following:

Entry/Exit Tracking

DHS has no effective system to determine whether non-citizens who legally enter the country subsequently leave it. Many aliens enter under temporary visas and then fail to leave after their visa expiration date ("visa overstays"). Prior efforts to track these visitors have proved to be ineffective. The US-VISIT system is intended to solve the problems that have plagued previous efforts. DHS OIG will monitor the system's establishment and independently assess its effectiveness.

Student Visa Tracking

DOJ developed and fielded the Student and Exchange Visitor Information System (SEVIS), an automatic tracking system designed to improve the monitoring of foreign students while in the United States. DOJ OIG identified computer difficulties SEVIS experienced, and serious shortcomings in the school accreditation process. Recent statements from various higher education officials indicate that problems persist.

Interior Enforcement/ Detection

Apprehension, detention, and removal of illegal aliens is a key DHS interior security enforcement responsibility. ICE uses several systems to perform its interior security enforcement role. These systems include SEVIS and the National Security Entry-Exit Registration System (to be replaced by US-VISIT). ICE uses the information the systems generate to locate and remove aliens who overstay their visas or otherwise violate the terms of their admission. DOJ OIG concluded in a pre-DHS study that, on average, ICE is deporting only about 13% of all non-detained aliens under final orders of removal. The study

also sampled high risk categories and found that ICE had removed only 6% of aliens with final removal orders who came from countries listed as sponsors of terrorism. And, only 35% of aliens with criminal records and final removal orders were being removed.

ICE has other interior enforcement responsibilities that include investigating a range of issues like terrorist financing, export enforcement, money laundering, intellectual property rights violations, preventing the illegal employment of undocumented aliens, and attacking sweatshops and smuggling enterprises that exploit undocumented aliens.

The DHS OIG is currently reviewing ICE's detention of illegal aliens, focusing on whether ICE has sufficient resources and facilities to house detainees. In addition, we have incorporated other projects into our FY04 Performance Plan, which will evaluate the effectiveness of ICE's Institutional Removal Program and the practices and procedures ICE uses to prioritize aliens to be detained.

Intelligence Matters

One of the principal objectives behind the establishment of DHS was to centralize in its Information Analysis and Infrastructure Protection (IAIP) directorate intelligence concerning terrorist threats against the homeland, so as to facilitate analysis and appropriate follow up action. However, since the establishment of DHS, two even newer entities, the Terrorist Threat Integration Center, run by the CIA, and the Terrorist Screening Center, run by the Federal Bureau of Investigation (FBI), have been created that have homeland security related intelligence responsibilities that either overlap with, duplicate, or even trump those of IAIP. Ensuring that DHS has access to the intelligence that it needs to prevent and/or respond to terrorist threats is, under such circumstances, an even harder challenge than it would otherwise be.

Moreover, the federal government's various terrorist watchlists have yet to be integrated into a single one for easy access by border security officials and law enforcement personnel. DHS OIG is monitoring DHS' terrorist watchlist integration efforts.

In addition to the foregoing, insufficient staff, slower than anticipated consolidation of administration functions, office locations, and delayed connectivity with other agency databases and communication systems have further hampered IAIP's and, therefore, DHS' effectiveness with regard to intelligence related matters.

Integrated Fingerprint Systems

CBP uses a two-print fingerprint scanning and automated search system (IDENT) to identify repeat illegal entries by aliens and to conduct a criminal history check against a limited immigration database. The DOJ has worked for several years to integrate IDENT with the FBI's Integrated Automated Fingerprint Identification System, which is a ten-print full criminal history check. This integration is critical to identifying illegally entering aliens on lookout lists or with criminal histories, but progress has been slow. According to the latest

DOJ OIG report, the initial integrated version is scheduled for deployment this month, two years later than originally planned.

High Technology Equipment

Since September 11, 2001, CBP has expanded the use of high-technology equipment to search for radioactive materials, explosives, and chemicals. This equipment, which includes various vehicle x-ray systems, radiation detection systems, and trace detection systems, permits CBP officials to inspect cargo and conveyances for weapons of mass destruction without having to undertake the costly and time-consuming process of unloading cargo, drilling through it, or dismantling conveyances.

Treasury OIG concluded that it was unable to determine whether use of detection equipment was meeting legacy U.S. Customs Service's goals. According to Treasury OIG, the efficient and effective use and deployment of high-technology equipment could be improved through decisive management action. The DHS OIG will continue to examine deployment strategies, equipment utilization, reliability testing, and establishment of performance measures to assess the effectiveness of high technology equipment in detecting weapons of mass destruction.

TRANSPORTATION SECURITY

Screeners

The Aviation and Transportation Security Act (ATSA), which was enacted as a result of the events of September 11, 2001, mandated that 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. In the rush to meet the statutory deadline, TSA fell short in a number of areas, including screener recruitment, training, and performance. While some improvements have been made, further improvements are necessary to ensure that the flying public is adequately protected from terrorist activity. For example, a recent DHS OIG undercover audit of screener procedures revealed vulnerabilities and the need for full development of supervisory training programs. The DHS OIG is evaluating TSA's revised training programs and will continue to monitor TSA's progress in improving its weapons detection performance.

Checking Bags 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). 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 where needed (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. DHS OIG is conducting reviews of EDS equipment deployment, and contract oversight and performance with regard to training, maintenance, and reliability of such equipment.

Maritime Security

Management challenges concerning the implementation of the Maritime Transportation Security Act of 2002 include the approval and enforcement of about 18,000 vessel, facility, and port security plans to be submitted by all owner/operators by December 31, 2003, under the guidance of the U.S. Coast Guard. Maritime Security final rules issued by the U.S. Coast Guard in mid-October 2003 established compliance dates and documentation requirements for owners and operators, who have until July 1, 2004, to implement vessel and facility security plans fully. The Coast Guard is also responsible for developing Area Maritime Security Plans, which must be consistent with the department's National Maritime Transportation Security Plan. These security plans will contribute to DHS' efforts to assess facility and vessel vulnerability and in the establishment of security incident response plans.

As a result of the events of September 11, 2001, seaport security and the cargo that enters into the U.S. at our seaports have become prominent issues. While CBP has taken positive steps to address the terrorist threat, additional steps are needed. Treasury OIG found that, to mitigate vulnerabilities at U.S. ports of entry, CBP must strengthen its implementation of security controls and procedures. Additionally, improvements in staffing, training, and proper record keeping are needed to enhance targeting effectiveness. Further, the commonality of conditions identified at the ports visited indicated that closer oversight and direction by Customs headquarters management was needed to ensure that vessel containers were effectively secured, inspected, and targeted for inspection.

CBP has implemented initiatives to increase the involvement of industry in the area of port security to reduce the vulnerability of U.S. ports to terrorist activities. These initiatives include the Container Security Initiative (CSI), and the Customs Trade Partnership Against Terrorism (C-TPAT). Another initiative is to improve the Automated Targeting System by revising rules and rule weights to enhance capabilities for identifying cargo that might conceal weapons of mass destruction and other implements of terrorism. DHS OIG is currently reviewing the CBP's inspection process and conducting an audit of CSI, focusing on the issues associated with the pre-screening element, such as reliance on inspections of cargo containers conducted by foreign officials. We also plan to review C-TPAT to determine whether CBP has implemented adequate management controls over the program to ensure that participants are meeting program requirements and program objectives.

Treasury OIG also found that the significant safety, smuggling, and terrorism risks associated with the importation of hazardous materials (HAZMAT) require CBP to strengthen its management controls. CBP needs to focus on allocation of HAZMAT resources and identification of shipments at highest risk for smuggling drugs or becoming implements of terrorism.

Other Transportation Modes

Appropriately, TSA focused its first year efforts on aviation security. However, ATSA mandates that TSA be responsible for security in all modes of transportation, including non-aviation modes such as rail, highway, mass transit, cruise lines, and ferries. TSA has to date given relatively little attention to other modes. TSA is in the process of working on a national security plan that will address all modes of transportation, and of drafting memorandums of understanding with various Transportation Department agencies to determine how they will coordinate work in the future. DHS OIG will examine whether TSA devotes appropriate resources and efforts to non-aviation modes of transportation.

INTEGRATION OF INFORMATION SYSTEMS

Information technology remains a major management challenge for DHS. The Chief Information Officer (CIO) is working to establish a department-wide IT infrastructure for effective communications and information exchange among DHS employees. In this context, the CIO is charged with inventorying IT assets, identifying wireless compatibilities, and consolidating hundreds of redundant systems from the legacy agencies into a modernized, interoperable, and integrated infrastructure that supports the mission and business processes of DHS. Additionally, operational IT planning and budgeting must align with mission goals, reflect federal budgetary constraints, and utilize capital asset planning techniques to ensure that the technology portfolio achieves performance goals with the lowest life cycle costs and with the least risk.

SECURITY OF INFORMATION TECHNOLOGY INFRASTRUCTURE

The security of IT infrastructure is also 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 management program that addresses the risks and vulnerabilities facing DHS' IT systems. As DHS OIG reported in September 2003, based on its annual FISMA evaluation, DHS has made some progress in establishing a framework for an IT systems security program in the short time since its inception. However, still more needs to be done. For example, DHS does not have a process to ensure that all security weaknesses, for both classified and unclassified systems, are identified and remedied. Further, none of the DHS components has a fully functioning IT security program.